Dell™ PowerConnect™ 6024/6024F Systems

User's Guide

Notes, Notices, and Cautions

NOTE: A NOTE indicates important information that helps you make better use of your computer.

NOTICE: A NOTICE indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A CAUTION indicates a potential for property damage, personal injury, or death.

April 2005 Rev A04

Contents

6 Configuring System Information

8 Configuring Routing

9 Viewing Statistics

10 Configuring Quality of Service

11 Getting Help

1

Introduction

NOTICE: Before proceeding, read the release notes for this product. You can download the release notes from support.dell.com.

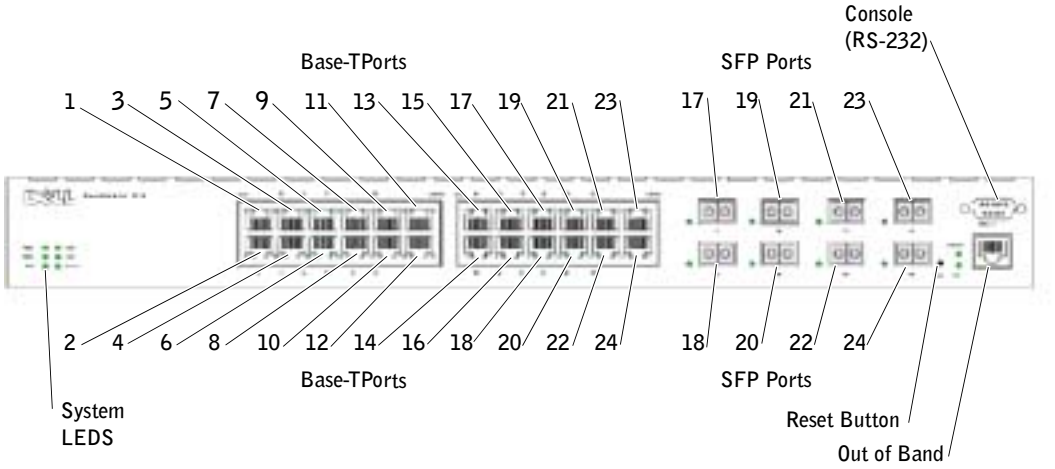
The Dell™ PowerConnect™ 6024/6024F is a standalone Layer 3 switch that extends the Dell PowerConnect LAN switching product range. The switch includes the following features:

- 1U form factor, rack-mountable chassis design
- Out-of-band management port for RJ-45 and RS-232 connections.
- Support for all data-communication requirements for a multi-layer switch, including a full suite of Layer 2, Layer 3+, security, and management features.
- High availability with hot swappable power supplies and cooling fans

PowerConnect 6024

The PowerConnect 6024 provides 24 10/100/1000 Base-T RJ-45 ports with eight SFP combo ports that have an auto-sensing mode for speed, flow control, and duplex mode. SFP transceivers are sold separately.

Figure 1-1. PowerConnect 6024

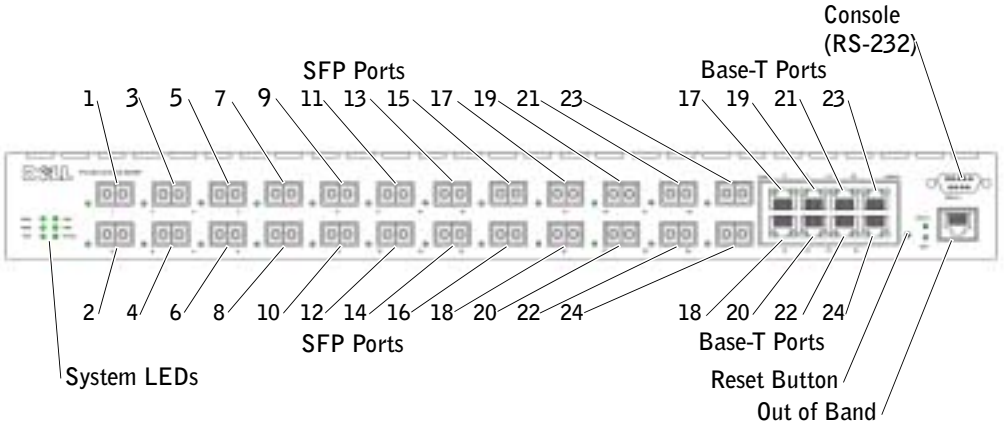


PowerConnect 6024F

PowerConnect 6024F provides 24 SFP ports with 8 10/100/1000 Base-T RJ-45 combo ports that have an auto-sensing mode for speed, flow control, and duplex mode. SFP transceivers are sold separately.

Figure 1-2. PowerConnect 6024F

CLI Documentation



The *CLI Reference Guide* provides information about the CLI commands used to configure the switch. The document provides CLI descriptions, syntax, and default values.

Features

This section describes the switch's user-configurable features. For a list of all features, refer to the software version release notes.

Port Based Features

Virtual Cable Testing (VCT)

VCT detects and reports potential copper link cabling issues, such as cable opens or cable shorts.

Jumbo Frames Support

Jumbo frames enables transporting identical data in fewer frames to ensure less overhead, lower processing time, and fewer interrupts.

MDI/MDIX Support

Your switch supports auto-detection between crossed and straight-through cables.

Standard wiring for end stations is Media-Dependent Interface (MDI) and the standard wiring for hubs and switches is known as Media-Dependent Interface with Crossover (MDIX).

For information about configuring MDI/MDI for ports or LAGs, see "Defining Port Configuration" or "Defining LAG Configuration."

Hardware Watchdog Support

The switch uses Hardware Watchdog to detect issues and take corrective action when the software stops responding.

Auto Negotiation

Auto negotiation allows the device to advertise modes of operation. The auto negotiation function provides the means to exchange information between two devices that share a point-to-point link segment, and to automatically configure both devices to take maximum advantage of their transmission capabilities.

The PowerConnect 6024/6024F enhances auto negotiation by providing port advertisement. Port advertisement allows the system administrator to configure the port speeds advertised.

For information about auto negotiation, see "Defining Port Configuration" or "Defining LAG Configuration."

Flow Control Support (IEEE 802.3X)

Flow control enables lower speed devices to communicate with higher speed devices by requesting that the higher speed device refrains from sending packets. Transmissions are temporarily halted to prevent buffer overflows.

For information about configuring flow control for ports or LAGs, see "Defining Port Configuration" or "Defining LAG Configuration."

Head of Line Blocking Prevention

Head of Line (HOL) blocking prevents traffic delays and frame loss caused by traffic competing for the same egress port resources. HOL blocking queues packets, and the packets at the head of the queue are forwarded before packets at the end of the queue.

Back Pressure Support

On half-duplex links, a receiver may prevent buffer overflows by occupying the link so that it is unavailable for additional traffic.

For information about configuring Back Pressure for ports or LAGs, see "Defining Port Configuration" or "Defining LAG Configuration."

MAC Address Supported Features

MAC Address Support

The switch supports up to 16K MAC addresses and reserves specific MAC addresses for system use.

Self-Learning MAC Addresses

The switch enables MAC addresses to be automatically learned from incoming packets.

Automatic Aging for MAC Addresses

MAC addresses that have not seen any traffic for a given period are aged out, which prevents the Bridging Table from overflowing.

For information about configuring the MAC Address age-out period, see "Viewing Dynamic Addresses."

Static MAC Entries

User-defined MAC entries are stored in the Bridging Table with the self-learned addresses.

For information about configuring the static MAC addresses, see "Defining Static Addresses."

VLAN-Aware MAC-based Switching

Packets arriving from an unknown source address are sent to the CPU and added to the Hardware Table. Future Packets addressed to or from this address are more efficiently forwarded.

MAC Multicast Support

Multicast service is a limited broadcast service that allows one-to-many and many-to-many connections. In Layer 2 multicast services, a single frame addressed to a specific multicast address is received, and copies of the frame to be transmitted on each relevant port are created.

For information about configuring MAC Multicast Support, see "Multicast Forwarding Support."

Layer 2 Features

IGMP Snooping

IGMP Snooping examines the contents of IGMP frames when they are forwarded by the switch from stations to an upstream multicast router. Snooping enables the switch to identify stations interested in multicast sessions and which multicast routers are sending multicast frames.

For information about configuring IGMP Snooping, see "IGMP Snooping."

Port Mirroring

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port.

For information about configuring port mirroring, see "Defining Port Mirroring Sessions."

Broadcast Storm Control

When Layer 2 frames are forwarded, broadcast and multicast frames are flooded to all ports on the relevant VLAN. The flooding occupies bandwidth, and loads all nodes connected on all ports. Storm control limits the amount of multicast and broadcast frames accepted and forwarded by the switch.

For information about configuring storm control, see "Enabling Storm Control."

VLAN Supported Features

VLAN Support

VLANs are collections of switching ports that comprise a single broadcast domain. Packets are classified as belonging to a VLAN based on either the VLAN tag or a combination of the ingress port and packet contents. Packets sharing common attributes can be groups in the same VLAN.

For information about configuring VLANs, see "Configuring VLANs."

Port-Based VLANs

Port-based VLANs classify incoming packets to VLANs based on their ingress port.

For information about configuring VLANs, see "Configuring VLANs."

IEEE802.1V Protocol Based VLANs

VLAN classification rules are defined on data-link layer (Layer 2) protocol identification. Protocol-based VLANs are used for isolating Layer 2 traffic for differing Layer 3 protocols.

For information about defining Protocol Based VLANs, see "Defining VLAN Protocol Groups."

Full 802.1Q VLAN Tagging Compliance

IEEE 802.1Q defines an architecture for virtual bridged LANs, the services provided in VLANs, and the protocols and algorithms involved in the provision of these services.

This standard requires an ability to mark frames with a desired Class of Service (CoS) tag value (0-7).

GVRP Support

GARP VLAN Registration Protocol (GVRP) provides IEEE 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports. When GVRP is enabled, the switch registers and propagates VLAN membership on all ports that are part of the active underlying Spanning Tree protocol topology.

For information about configuring GVRP, see "Configuring GVRP. "

Private VLAN Edge

Private VLAN Edge (PVE) ports are a Layer 2 security feature that provides port-based security between adjacent ports within a VLAN. It is an extension of the common VLAN. Traffic from protected ports is sent only to the uplink ports and cannot be sent to other ports within the VLAN.

For information about configuring PVE ports, see "Configuring Ports".

Spanning Tree Protocol Features

Spanning Tree Protocol (STP) per Device

802.1d STP is a standard requirement of Layer 2 switches that allows bridges to automatically prevent and resolve L2 forwarding loops. Switches exchange configuration messages, using specifically formatted frames, and selectively enable and disable forwarding on ports.

For information about configuring STP, see "Configuring the Spanning Tree Protocol."

Fast Link

STP can take as long as 30-60 seconds to converge as it detects possible loops and allows time for status changes to propagate and for relevant devices to respond. This duration is considered too long for many applications. Fast Link bypasses this delay without requiring multiple data paths for network resiliency.

For information about enabling Fast Link for ports and LAGs, see "Defining Port Configuration" or "Defining LAG Configuration."

IEEE 802.1W Rapid Spanning Tree

Rapid Spanning Tree Protocol (RSTP) detects uses network topologies to enable faster convergence, without creating forwarding loops.

For information about enabling RSTP, see "Defining the Rapid Spanning Tree."

Multiple Spanning Tree

Multiple Spanning Tree (MSTP) operation maps VLANs into ST instances. MSTP provides a differing load balancing scenario. Packets assigned to various VLANs are transmitted along different paths within MSTP Regions (MST Regions). Regions are one or more interconnected MSTP bridges with identical MSTP settings. The standard lets administrators assign VLAN traffic to unique paths.

For more information about MSTP, see "Defining the Multiple Spanning Tree".

Link Aggregation

Link Aggregation

Up to seven ports can combine to form a single Link Aggregated Group (LAG). This enables fault tolerance protection from physical link disruption, higher bandwidth connections and improved bandwidth granularity.

A LAG is composed of ports of the same speed, set to full-duplex operation.

For information about configuring LAGs, see "Defining LAG Configuration."

Link Aggregation and LACP

LACP uses peer exchanges across links to determine, on an ongoing basis, the aggregation capability of various links, and continuously provides the maximum level of aggregation capability achievable between a given pair of systems. LACP automatically determines, configures, binds, and monitors the binding of ports to aggregators within the system.

For information about LACP, see "Defining LACP Parameters."

Routing Features

IP Routing

IP routing forwards to a next-hop device any packets that are addressed to the system MAC addresses but not to a system IP address.

For information about configuring IP routing, see "Configuring Global IP Routing."

RIP Versions 1 and 2

Routing Information Protocol (RIP) is a distance-vector routing protocol. RIP selects routes based on the hop count to the destination. RIP 2 enhances the efficiency, usability, and authentication methods of the RIP protocol.

For information about configuring RIP, see "Configuring RIP."

OSPF Version 2

Open Shortest Path First (OSPF) is an internal gateway routing protocol. In networks with a large number of inter-connected routers, OSPF is more efficient than RIP because OSPF uses less link bandwidth and converges more quickly.

For information about configuring OSPF, see "Configuring OSPF Parameters and Filters."

Address Resolution Protocol (ARP)

In IP routing, routers and Layer 3 switches use various routing protocols to discover network topology and define routing tables. ARP automatically determines Device Next-Hop MAC addresses of systems, including directly attached end systems. Users can override and supplement this by defining additional ARP table entries.

For information about configuring ARP, see "Defining ARP Settings."

ICMP Messages

Internet Control Message Protocol (ICMP) messages are used for out-of-band messages related to network operation or malfunction.

IGMPv2

IGMP enables the router to send IGMP queries in the form of L2 broadcasts over each interface. When a multicast packet is sent, and it has a multicast destination MAC address, all hosts on that router interface receive a copy. Hosts listen to all IGMP reports. If interested multicast groups have already been requested by any station on the same interface, the remaining stations do not send duplicate requests.

For information about configuring IGMP, see "Defining IGMP Interface Parameters."

Longest Prefix Match Support

Longest prefix matches are used primarily to determine the best next-hop route for a packet based solely on the destination address contained in the packet header. Because IP addresses are generally assigned in a manner that reflects the topology of the network, the result of a longest prefix match usually reflects the shortest route to the destination.

DVMRP

Distance Vector Multicast Routing Protocol (DVMRP) advertises the shortest-path routes to multicasting source networks with hosts that can transmit multicast IP traffic.

For information about configuring DVMRP, see "Configuring DVMRP Interfaces."

VRRP

Virtual Router Redundancy Protocol (VRRP) eliminates single points of failure in the routing environment. VRRP uses an election protocol that dynamically assigns responsibility for the virtual router to one of the VRRP routers in the LAN.

The election process provides dynamic failover in the forwarding responsibility, if the master is unavailable. Any virtual router IP address can be used as a default first-hop router by end-hosts.

For information about configuring VRRP, see "Configuring VRRP."

Layer 3 Features

TCP

Transport Control Protocol (TCP) connections are defined between 2 ports by an initial synchronization exchange. TCP ports are identified by an IP address and a 16-bit port number. Octets streams are divided into TCP packets, each carrying a sequence number.

UDP Relay

UDP Relay enables the device to forward specific UDP broadcasts from one interface to another. IP broadcast packets from one interface are not generally forwarded to another interface. However, some applications use UDP broadcast to detect the availability of a service. Other services require UDP broadcast packets to be routed to provide services to clients on another subnet.

BootP and DHCP Clients

DHCP enables additional setup parameters to be received from a network server upon system startup. DHCP service is an on-going process. DHCP is an extension to BootP.

For information about DHCP, see "Defining DHCP IP Interface Parameters."

BootP Relay

BootP enables a device to solicit and receive configuration data from servers. If the intended BootP server is not directly attached to a client's broadcast domain, a BootP relay service enables the client to reach the server.

DHCP Relay

DHCP enables a device to solicit and receive configuration data from servers. If the intended DHCP server is not directly attached to a client's broadcast domain, a DHCP relay service enables the client to reach the server.

For information about configuring DHCP Relay parameters, see "Defining DHCP Relay Parameters."

Quality of Service Features

Quality of Service (QoS) Support

To overcome unpredictable network traffic and optimize performance, you can apply Quality of Service (QoS) throughout the network to ensure that network traffic is prioritized according to specific criteria. Your switch supports two modes of QoS: basic and advanced.

Class Of Service 802.1p Support

The IEEE 802.1p signaling technique is an OSI Layer 2 standard for tagging and prioritizing network traffic at the data link/MAC sub-layer. The 802.1p traffic is classified and sent to the destination; no bandwidth reservations or limits are established or enforced. The 802.1p standard establishes eight levels of priority, similar to the IP Precedence IP Header bit-field.

Quality of Service Basic Mode

In basic QoS mode, it is possible to activate a trust mode (to trust VPT, DSCP, TCP/UDP or none). In addition, a single access control list can be attached to an interface.

For information about enabling QoS Basic Mode, see "Configuring Basic QoS Mode."

Quality of Service Advanced Mode

Advanced Quality of Service mode specifies flow classification and assigns rule actions that relate to bandwidth management. These rules can be grouped into a policy, which can be applied to an interface.

For information about enabling QoS Advanced Mode, see "Configuring Advanced QoS Mode."

Device Management Features

SNMP Alarms and Trap Logs

The system logs events with severity codes and timestamps. The events are sent as SNMP traps to a trap recipient list.

For information about SNMP Alarms and Traps, see "Defining SNMP Parameters."

Web Based Management

You can manage the system from any web browser. The switch contains an embedded web server that serves HTML pages that you can use to monitor and configure the system.

Configuration File Download

The switch's configuration file includes both system-wide and port-specific device configuration data. You can display configuration files through CLI commands.

For information about downloading configuration files, see "Downloading Files."

Software Download

Software download enables storage of backup firmware images. For information about downloading the software, see "Software Download and Reboot."

Trivial File Transfer Protocol (TFTP)

PowerConnect 6024/6024F supports boot image, firmware and configuration upload/download via TFTP.

Remote Monitoring

Remote monitoring (RMON) is an extension to the SNMP that provides comprehensive network *traffic* monitoring capabilities (as opposed to SNMP, which allows network *device* management and monitoring). RMON is a standard MIB that defines current and historical MAC-layer statistics and control objects, allowing real-time information to be captured across the entire network.

For information about RMON, see "Viewing RMON Statistics."

Simple Network Management Protocol (SNMP) Versions 1, 2 and 3

To control access to the system, a list of community entries is defined, each of which consists of a community string and its access privileges. There are three levels of SNMP security — read-only, read-write, and super. Only a super-user can access the community table itself.

Command Line Interface

Command Line Interface (CLI) syntax and semantics conform as much as possible to common industry practice. CLI is composed of mandatory and optional elements. Context-sensitive help provides format and value ranges allowed for current commands, and the CLI interpreter provides command and keyword completion.

Syslog

Syslog is a protocol that allows event notifications to be sent to a set of desired remote servers where they can be stored, examined, and acted upon.

For information about Syslog, see "Managing Logs."

SNTP

The Simple Network Time Protocol (SNTP) assures accurate network switch clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server.

For more information about SNTP, see "Configuring SNTP Settings."

Traceroute

Traceroute enables discovering IP routes that packets were forwarded along during the forwarding process. The CLI Traceroute utility can be executed from either User EXEC or Privileged EXEC modes.

Out-of-Band Management Port Support

An out-of-band management port is an external Ethernet port that carries only traffic between the system-administrator and the management applications. The out-of-band management port provides a physically secure link and also offers fault tolerance.

Security Features

Access Control Lists (ACL)

ACL provides rules for forwarding or blocking network traffic. You can define ACLs to enforce security enhancements by defining classification rules and assigning an action per rule. You can assign an ACL to an ingress interface (port or VLAN).

For information about defining ACLs, see "Defining IP based ACLs" and "Defining MAC based ACLs."

Port Based Authentication (802.1x)

Port based authentication enables authenticating system users on a per port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the Remote Authentication Dial In User Service (RADIUS) server using the Extensible Authentication Protocol (EAP).

For more information, see "Configuring Port Based Authentication."

Locked Port Support

Locked port limits access on a port only to users with specific MAC addresses. These addresses are manually defined or learned on that port. When a frame is seen on a locked port, and the frame source MAC address is not tied to that port, the protection mechanism is invoked.

For information about enabling locked port security, see "Configuring Port Security."

Password Management Security

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS and SNMP access are assigned security features.

For more information about password management, see "Managing Passwords".

TACACS+

TACACS+ provides centralized security for validation of users accessing the switch. TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes.

For information about defining TACACS+ settings, see "Configuring Out-of-Band TACACS+ Servers" and "Configuring TACACS+ Settings."

RADIUS Client

RADIUS is a client/server-based protocol in which the server maintains a user database, that contains per-user authentication information, such as user name, password and accounting information.

For information about defining RADIUS settings, see "Configuring RADIUS Settings."

SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. This connection provides functionality that is similar to an inbound telnet connection.

2

Hardware Description

This section contains information about device characteristics and module hardware configurations.

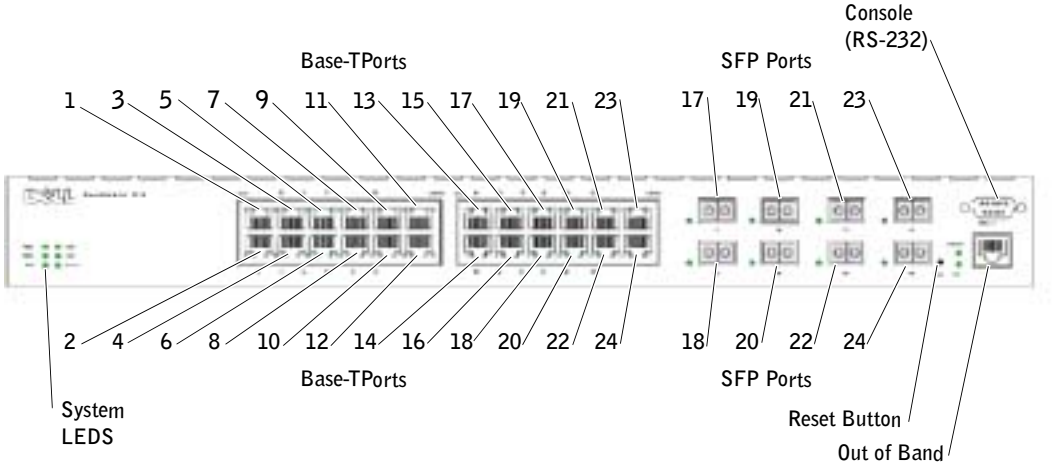
Ports Description

PowerConnect 6024

Ports 1-16 are designated as 10/100/1000 ports, and ports 17-24 are designated as combo ports. The port numbers are shown in the figure below.

A combo port is a single logical port with two physical connections — an RJ-45 connection and a SFP connection. When a connector is inserted in the SFP port, the SFP port is active, unless a Base-T port copper connector of the of the same number is inserted and has a link.

Figure 2-1. PowerConnect 6024 with 24 10/100/1000 Base-T Ports



The switch automatically detects the difference between crossed and straight through cables on RJ-45 ports. SFP ports support both SX and LX modules.

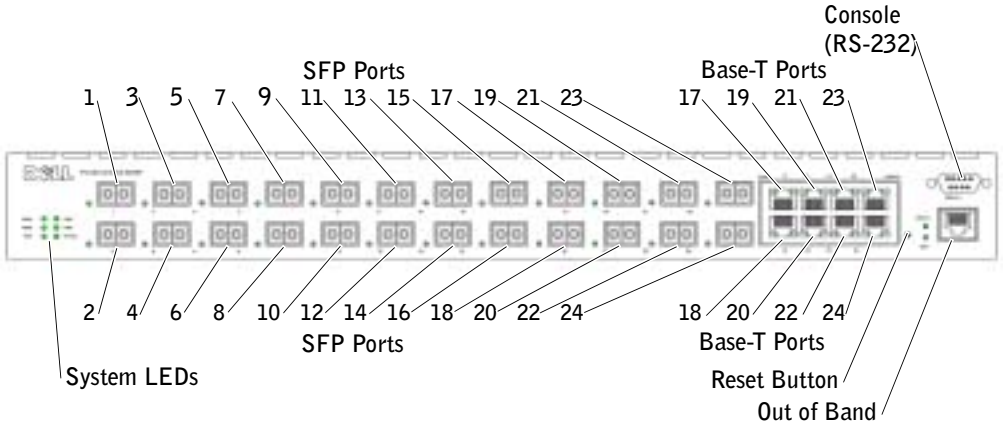
RJ-45 ports support half- and full-duplex mode 10/100/1000 Mbps.

PowerConnect 6024F

The PowerConnect 6024F ports differ from the PowerConnect 6024 only in port designation: Ports 1-16 are designated as SFP ports, and ports 17-24 are designated as combo ports. The port numbers are shown in the figure below.

For information about how the ports function, see the port description for the PowerConnect 6024.

Figure 2-2. PowerConnect 6024F with 24 SFP Ports



Out-of-Band Management Port

The Out-of-Band (OOB) management port is a 10/100 Mbps Ethernet port that you can use to connect directly to the switch to perform system administrator management applications. The Out-of-Band port is regarded as a regular IP interface to the system, and all management interfaces are available over this port.

For more information about configuring Out-of-Band, see "Out-of-Band Management Port."

Console (RS-232) Port

The console (RS-232) port is used only for management via a serial interface. This port is a direct connection to the switch, used to access CLI from a console terminal connected to an EIA/TIA-232 port.

The console port supports synchronous data of eight data bits, one stop bit, and no parity bit. The default baud rate is 115,200 bps.

Hardware Components

Physical Dimensions

The switch has the following physical dimensions:

- 440 x 460 x 44 mm (W x D x H).
- 17.32 x 18.11 x 1.73 inch (W x D x H).

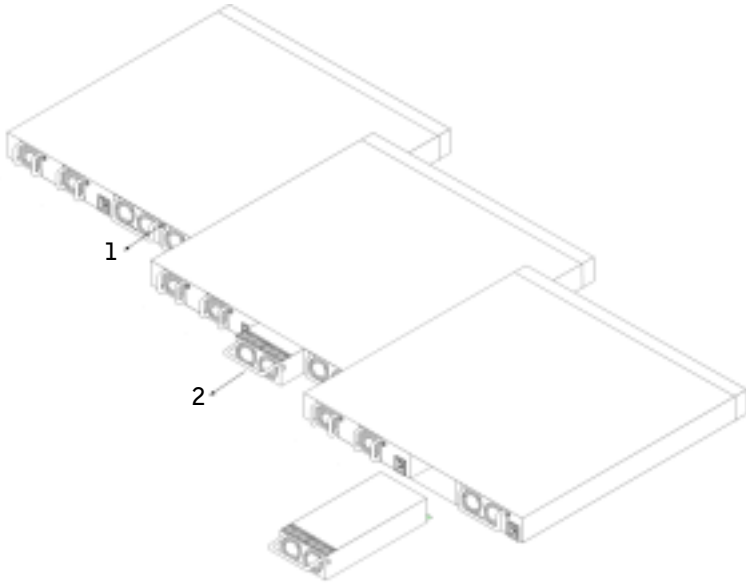
Power Supplies

Your switch is shipped with two internal power supplies. You can verify operation by observing the LEDs. See "System LEDs" for information.

To replace a power supply:

1. Remove the faulty power supply unit by removing its screw in the back panel and pulling it out.
2. Insert a new power supply into the slot, ensuring that the power supply is inserted fully into the switch.

Figure 2-3. Power Supply Insertion



3. Insert and tighten the screw to the power supply.
4. Connect each power supply to a different external power source.

When you connect to a different power source, the probability of the switch failing in the event of a power outage decreases.

Reset Button

The reset button, located on the front panel, manually resets the switch.

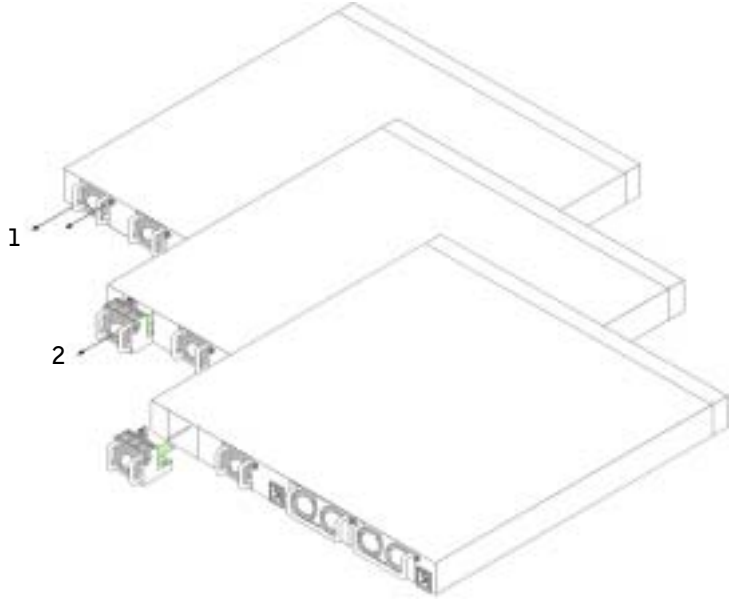
Ventilation System

There are two fans in the system. You can verify operation by observing the LEDs. See "System LEDs" for information.

To replace a fan:

1. Remove the two screws, and gently pull out the faulty fan.
2. Carefully insert the new fan into the slot.

Figure 2-4. Fan Installment/Replacement



3. Insert and tighten the screw to the fan.

LED Definitions

The front panel contains light emitting diodes (LED) that indicate the status of links, power supplies, fans, and system diagnostics.

SFP Port LEDs

Figure 2-5 illustrates the SFP port LEDs that are next to each SFP port.

Figure 2-5. SFP Port LEDs

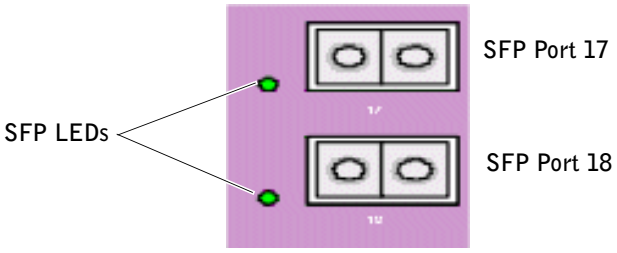


Table 2-1 contains SFP port LED definitions:

Table 2-1. SFP Port LEDs Definitions

LED	Color	Definition
SFP	Green	The port is currently linked.
	Flashing Green	The port is currently sending and/or receiving network traffic.
	Off	The port is currently not linked.

10/100/1000 Base-T Port LEDs

Each 10/100/1000 Base-T port has two LEDs. The speed LED is located on the left side of the port, while the link/duplex/activity LED is located on the right side. The following figure illustrates the 10/100/100 Base-T port LEDs:

Figure 2-6. 10/100/1000 Base-T Port LEDs

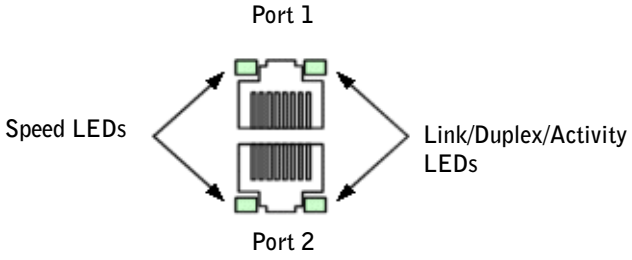


Table 2-2 contains 10/100/1000 Base-T port LED definitions.

Table 2-2. 10/100/1000 Base-T Port Definitions

LED	Color	Definition
Speed		
	Green	The port is operating at 1000 Mbps.
	Amber	The port is operating at 100 Mbps.
	Off	The port is operating at 10 Mbps.
Link		
	Green	The port is running, and the full duplex mode is active.
	Flashing Green	The port is sending or receiving packets, and running full duplex mode.
	Amber	The port is running, and the half duplex mode is active.
	Flashing Amber	The port is sending or receiving packets, and running half duplex mode.
	Off	The port is not linked.

System LEDs

The system LEDs, located on the left side of the front panel, provide information about the power supplies, fans, thermal conditions, and diagnostics.

Figure 2-7 illustrates the System LEDs.

Figure 2-7. System LEDs

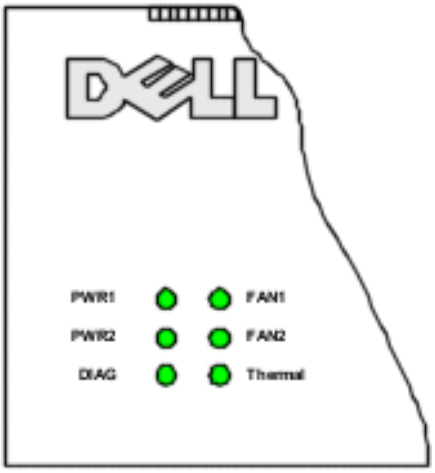


Table 2-3 contains system LED definitions.

Table 2-3. System LED Definitions

LED	Color	Definition
Fan 1		
	Green	Fan 1 is present and operating.
	Red	Fan 1 is present, but not operating.
	Off	Fan 1 is not present.
Fan 2		
	Green	Fan 2 is present and operating.
	Red	Fan 2 is present, but not operating.
	Off	Fan 2 is not present.
PWR1		
	Green	Power Supply 1 is present and operating.
	Red	Power Supply 1 is present, but not operating.
	Off	Power Supply 1 is not present.

Table 2-3. System LED Definitions

LED	Color	Definition
PWR2		
	Green	Power Supply 2 is present and operating.
	Red	Power Supply 2 is present, but not operating.
	Off	Power Supply 2 is not present.
Dia (Diagnostic)		
	Flashing Green	A diagnostics test is currently in progress.
	Green	The diagnostics test was successfully completed.
	Red	The diagnostics test failed.
Thermal		
	Red	The system has exceeded the maximum temperature.
	Off	The system temperature is normal.

3

Cable, Port, and Pinout Information

This section describes the switch's physical interfaces and provides information about cable connections.

Stations are connected to the switch's ports through the physical interface ports on the front panel. For each station, the appropriate mode (Half/Full Duplex, Auto) is set.

Pin Connections for the 10/100/1000 Ethernet Interface

The switching port can connect to stations wired in standard RJ-45 Ethernet station mode using straight cables. Transmission devices connected to each other use crossed cables.

Figure 3-1 illustrates the RJ-45 pins, and Table 3-1 contains the RJ-45 pin allocations.

Figure 3-1. RJ-45 Connector

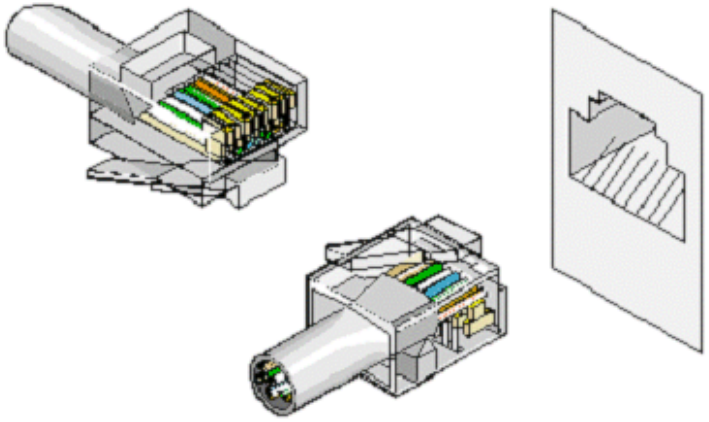


Table 3-1. RJ-45 Pin Connections for 10/100/1000 Base T

Pin	Use
1	TxRx 1+
2	TxRx 1-
3	TxRx 2+

Table 3-1. RJ-45 Pin Connections for 10/100/1000 Base T

Pin	Use
4	TxRx 2-
5	TxRx3+
6	TxRx 3-
7	TxRx 4+
8	TxRx 4-

Pin Connections for SFP Interfaces

Figure 3-2 illustrates an SFP connector, and Table 3-2 shows the pin assignments for an optional SFP connector.

Figure 3-2. SFP Connector

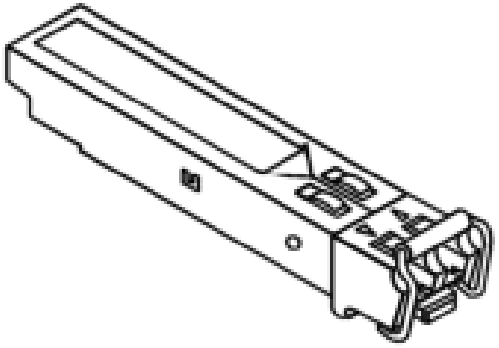


Table 3-2. SFP Pin Connections

Pin	Use
1	Transmitter ground (common with receiver ground)
2	Transmitter fault
3	Transmitter disable; laser output disabled on high or open
4	Module definition 2; data line for serial ID.
5	Module definition 1; clock line for serial ID.

Table 3-2. SFP Pin Connections

Pin	Use
6	Module definition 0; grounded within the module
7	Rate select; no connection required.
8	Loss of signal indication; logic 0 indicates normal operation.
9	Receiver ground (common with transmitter ground)
10	Receiver ground (common with transmitter ground)
11	Receiver ground (common with transmitter ground)
12	Receiver inverted data out; AC coupled.
13	Receiver non-inverted data out; AC coupled.
14	Receiver ground (common with transmitter ground)
15	Receiver power supply
16	Transmitter power supply
17	Transmitter ground (common with receiver ground)
18	Transmitter non-inverted data in
19	Transmitter inverted data in
20	Transmitter ground (common with receiver ground).

Serial Cable Connection

You can use serial cables (null-modem) to connect the switch to a terminal for initial setup and configuration (You can also use a PC running terminal emulation software.). The switch's serial cable is female to female DB-9 crossover cable (see Figure 3-3).

Figure 3-3 shows the serial cable and Table 3-3 shows the serial connector pin assignments.

Figure 3-3. Serial Connector

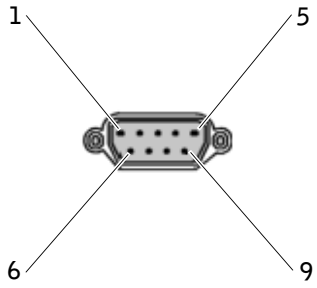


Table 3-3 contains serial cable pin assignments.

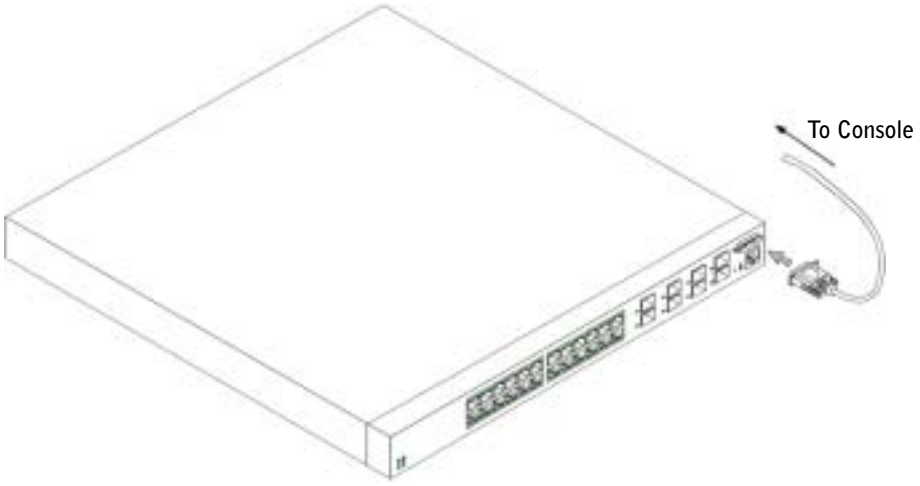
Table 3-3. Serial Connector Pin Assignment

Signal	Pin	Management Console Port Signal
Unused	1	Unused
TXD	2	TXD
RXD	3	RXD
Unused	4	RXD
GND	5	GND
Unused	6	Unused
CTS	7	CTS
RTS	8	RTS
Unused	9	Unused

Connecting the Switch to a Terminal

1. Connect the null modem (serial) cable to the terminal (console) ASCII DTE RS-232 connection.
2. Connect the interface cable to the switch's serial port connection (see Figure 3-4).

Figure 3-4. Serial Connection to Switch



AC Power Connection

1. Using a 5-foot (1.5 m) standard power cable with safety ground connected, connect the power cable to the AC main socket located on the rear panel (see Figure 3-5).
2. Connect the power cable to a grounded AC outlet.

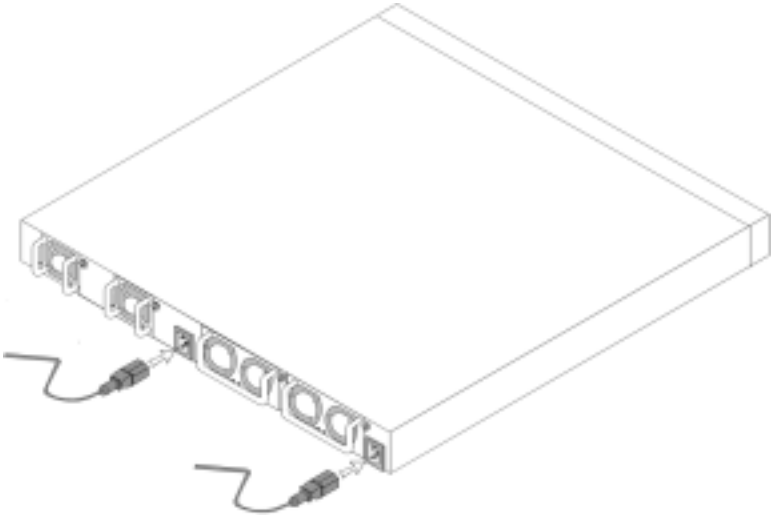
NOTE: It is recommended that you connect the second power supply to a different power source.

3. Confirm that the device is connected and operating correctly by examining the LEDs on the front and rear panel.

   For a complete explanation of the LEDs, see "Hardware Description."

4. Repeat the procedure for the second power supply.

Figure 3-5. AC Power Connection to Switch



4

Using Dell OpenManage Switch Administrator

Starting the Application

1. Open a web browser.
2. Enter the switch's IP address (as defined in the CLI) in the address bar and press <Enter>.

   For information about assigning an IP address to a switch, see "Initial Configuration."
3. When the **Enter Network Password** window displays, enter a user name and password.

NOTE: The switch is not configured with a default password, and you can configure the switch without entering a password. For information about recovering a lost password, see "Password Recovery."

NOTE: Passwords are both case sensitive and alpha-numeric.

4. Click **OK**.
5. The **Dell OpenManage Switch Administrator** home page displays.

Understanding the Interface

The home page (see Figure 4-1) contains the following views:

- **Tree view** — Located on the left side of the home page, the tree view provides an expandable view of features and their components.
- **Device view** — Located on the right side of the home page, the device view provides a view of the device, an information or table area, and configuration instructions.

Figure 4-1. Switch Administrator Components

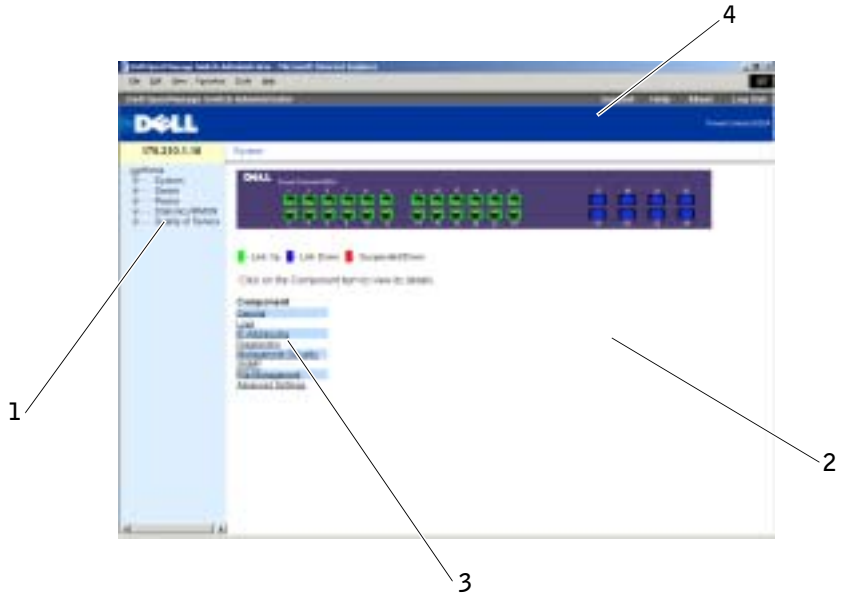


Table 4-1 lists the interface components with their corresponding numbers.

Table 4-1. Interface Components

Component	Name
1	The tree view contains a list of various device features. The branches in the tree view can be expanded to view all the components under a specific feature, or retracted to hide the feature's components. By dragging the vertical bar to the right, you can expand the tree area to view a full name of a component.

Table 4-1. Interface Components

Component	Name
2	The device view provides information about device ports, current configuration and status, table information, and feature components. The port coloring indicates if a port is currently active. Green indicates the port is enabled, red indicates that an error has occurred on the port, and blue indicates that the link is disabled. **NOTE:** The LEDs do not appear in the device view. You can only determine LED status by looking at the actual switch. For information about LEDs, see "LED Definitions." Depending on which option you select, the area at the bottom of the device view displays other device information and/or dialogs for configuring parameters.
3	The components list contains a list of feature components. You can also view components by expanding a feature in the tree view.
4	The information buttons provide access to information about the switch and access to Dell Support. For more information, see "Information Buttons."

Using the Switch Administrator Buttons

Information Buttons

Table 4-2. Information Buttons

Button	Description
Support	Opens the Dell Support page at **support.dell.com**
Help	Online help that contains information to assist in configuring and managing the switch. The online help pages are linked directly to the pages. For example, if the **IP Addressing** page is open, the help topic for that page displays if you click **Help**.

Table 4-2. Information Buttons

Button	Description
About	Contains the version and build number and Dell copyright information.
Log Out	Logs out of the application and closes the browser window.

Device Management Buttons

Table 4-3. Device Management Buttons

Button	Description
Apply Changes	Applies set changes to the device.
Add	Adds information to tables or dialogs.
Telnet	Starts a Telnet session.
Query	Queries tables.
Show All	Displays the device tables.
Left arrow/Right arrow	Moves information between lists.
Refresh	Refreshes device information.
Reset All Counters	Clears statistic counters.
Print	Prints the **Network Management System** page and/or table information.
Show Neighbor's Info	Displays the **Neighbors List** from the **Neighbors Table** page.
Draw	Creates statistics charts on-the-fly.
Clear Log	Clears log messages from the log buffer.
Reset	Resets the switch.
Test Now	Runs diagnostic test for copper cables.

Defining Fields

User-defined fields can contain 1-159 characters, unless otherwise noted on the Dell OpenManage Switch Administrator Web page.

All characters may be used except for the following:

- \
- /
- :

- *
- ?
- <
- >
- |

Accessing the Switch Through the CLI

The switch can be managed over a direct connection to the console port or via a Telnet connection. For information about out-of-band management ports, see "Out-of-Band Management Port."

Using the CLI is similar to entering commands on a Linux system. If access is via a Telnet connection, ensure the device has an IP address defined and that the workstation used to access the device is connected to the device prior to beginning using CLI commands.

For information about configuring an initial IP Address, see "Initial Configuration."

NOTE: Ensure the client is loaded, before using the CLI.

Console Connection

1. Power on the switch and wait until the startup is complete.
2. When the `Console>` prompt displays, type `enable` and press <Enter>.
3. Configure the device and enter the necessary commands to complete the required tasks.
4. When finished, exit the session with the `quit` or `exit` command.

NOTE: If a different user logs into the system in the Privilege EXEC command mode, the current user is logged off and the new user is logged in.

Telnet Connection

Telnet is a terminal emulation TCP/IP protocol. ASCII terminals can be virtually connected to the local device through a TCP/IP protocol network. Telnet is an alternative to a local login terminal where a remote login is required.

Your switch supports up to four simultaneous Telnet sessions. All CLI commands can be used over a telnet session.

To start a Telnet session:

1. Select **Start** > **Run**.
2. In the **Run** window, type `Telnet` *`<IP address>`* in the **Open** field.
3. Click **OK** to begin the Telnet session.

Using the CLI

Command Mode Overview

The CLI is divided into command modes. Each command mode has a specific command set. Entering a question mark at the console prompt displays a list of commands available for that particular command mode.

In each mode, a specific command is used to navigate from one command mode to another.

During the CLI session initialization, the CLI mode is the User EXEC mode. Only a limited subset of commands are available in the User EXEC mode. This level is reserved for tasks that do not change the console configuration and is used to access configuration sub-systems such as the CLI. To enter the next level, the Privileged EXEC mode, a password is required (if configured).

The Privileged EXEC mode provides access to the device global configuration. For specific global configurations within the device, enter the next level, Global Configuration mode. A password is not required.

The Global Configuration mode manages the device configuration on a global level.

The Interface Configuration mode configures the device at the physical interface level. Interface commands which require subcommands have another level called the Subinterface Configuration mode. A password is not required.

User EXEC Mode

After logging into the device, the EXEC command mode is enabled. The user-level prompt consists of the host name followed by the angle bracket (>). For example:

```
console>
```

NOTE: The default host name is `console` unless it has been modified during initial configuration.

The user EXEC commands permit connecting to remote devices, changing terminal settings on a temporary basis, performing basic tests, and listing system information.

To list the user EXEC commands, enter a question mark at the command prompt.

Privileged EXEC Mode

Privileged access can be protected to prevent unauthorized access and ensure operating parameters. Passwords are displayed on the screen, and are case sensitive.

To access and list the Privileged EXEC Mode commands:

1. At the prompt type `enable` and press <Enter>.
2. When a password prompt displays, enter the password and press <Enter>.

   The Privileged EXEC mode prompt displays as the device host name followed by #. For example:

   ```
   console#
   ```

To list the Privileged EXEC commands, type a question mark at the command prompt and press <Enter>.

To return from Privileged EXEC Mode to User EXEC Mode use any of the following commands: `disable`, `exit/end`, or <Ctrl><Z>.

The following example illustrates accessing privileged EXEC mode and then returning to the User EXEC mode:

```
console>enable
Enter Password: ******
console#
console#disable
console>
```

Use the **exit** command to move back to a previous mode. For example, you can move from Interface Configuration mode to Global Configuration mode, and from Global Configuration mode to Privileged EXEC mode.

Global Configuration Mode

Global Configuration commands apply to system features, rather than a specific protocol or interface.

To access Global Configuration mode, at the Privileged EXEC Mode prompt, type `configure` and press <Enter>. The Global Configuration Mode displays as the device host name followed by the pound sign # and (config).

```
console(config)#
```

To list the Global Configuration commands, enter a question mark at the command prompt.

To return from Global Configuration mode to Privileged EXEC mode, type the `exit` command or use the <Ctrl><Z> command.

The following example illustrates how to access *Global Configuration Mode* and return back to the *Privileged EXEC Mode*:

```
console#
console#configure
console(config)#exit
console#
```

Interface Configuration Mode

Interface configuration commands modify specific IP interface settings, including bridge-group, description, and so forth. The Interface Configuration modes are:

- **VLAN** — Contains commands to create and configure a VLAN as a whole, for example, to create a VLAN and apply an IP address to the VLAN.
- **Port Channel** — Contains commands for configuring Link Aggregation Groups (LAG).
- **IP** — Contains commands for managing IP interfaces.
- **Out-of-Band-Ethernet** — Contains commands for managing and configuring the management connections.

CLI Examples

CLI commands are provided as configuration examples. For a full description of the CLI commands, including examples, refer to your switch's *CLI Reference Guide*.

5

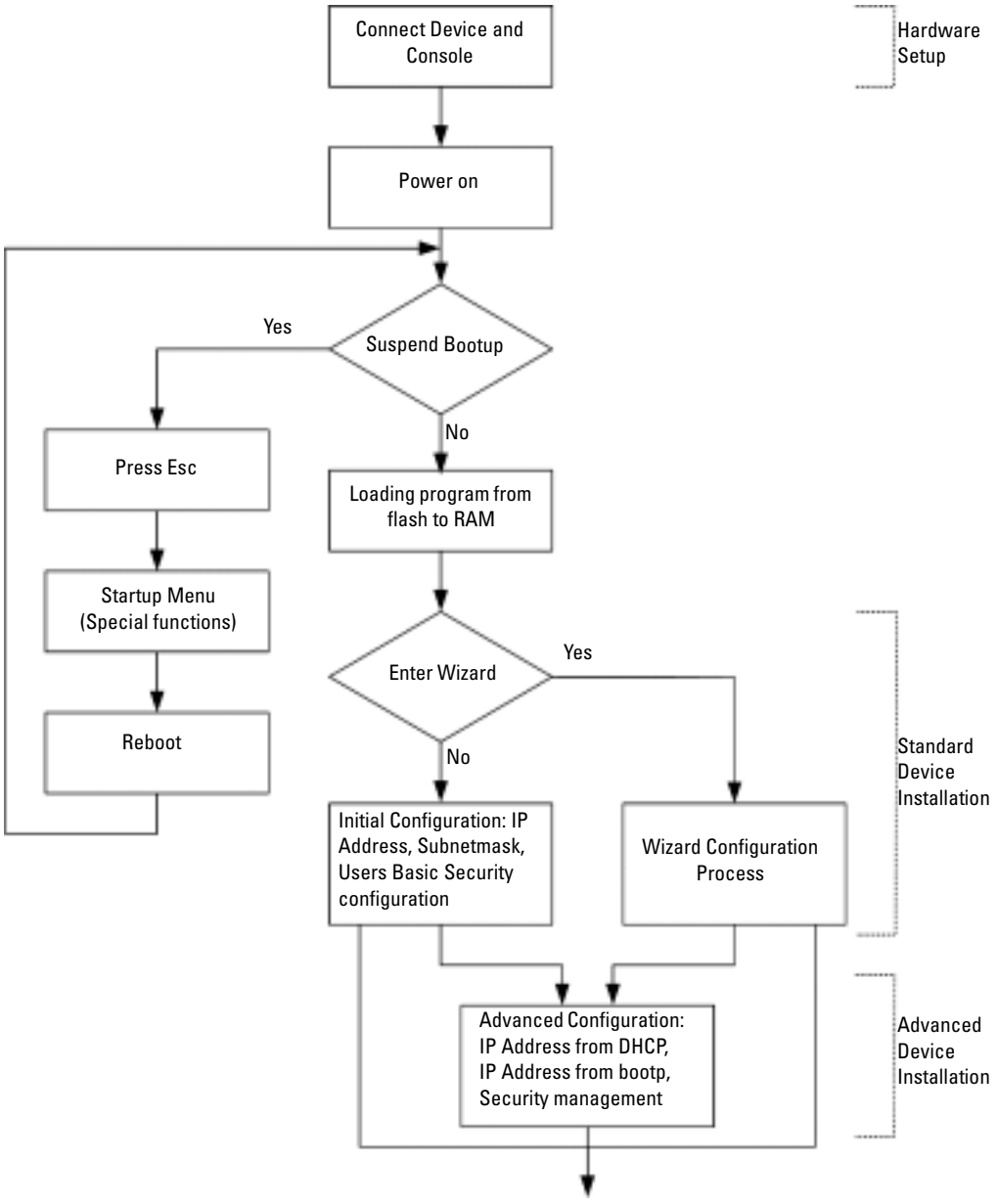
Configuring the Switch

This section describes the initial device configuration.

After completing all external connections, you must connect a terminal to the device to monitor the boot and other procedures. The order of installation and configuration procedures is illustrated in Figure 5-1. For the initial configuration, the standard device configuration is performed. You can perform other functions, but doing so suspends the installation process and causes a system reboot. Performing other functions is described later in this section.

NOTICE: Before proceeding, read the release notes for this product. You can download the release notes from **support.dell.com**.

Figure 5-1. Installation and Configuration Jobflow



General Configuration Information

Your switch has predefined features and setup configuration.

Auto-Negotiation

Auto-negotiation allows a device to advertise modes of operation and share information with another device that shares a point-to-point link segment. This automatically configures both devices to take maximum advantage of their abilities.

Auto-negotiation is performed completely within the physical layers during link initiation, without any additional overhead to either the MAC or higher protocol layers. Auto-negotiation allows the ports to do the following:

- Advertise their abilities
- Acknowledge receipt and understanding of common modes of operation that both devices share
- Reject the use of operational modes that are not shared by both devices
- Configure each port for the highest-level operational mode that both ports can support

If connecting a port of the switch to the network interface card (NIC) of a workstation or server that does not support auto-negotiation or is not set to auto-negotiation, both the switching port and the NIC must be manuallyet with the Web browser interface or CLI commands to the same speed and duplex mode.

NOTICE: If the station on the other side of the link attempts to auto-negotiate with a port that is manually configured to full duplex, the auto-negotiation results in the station attempting to operate in half duplex. The resulting mismatch may lead to significant frame loss. This is inherent in the auto-negotiation standard.

Switching Port Default Settings

The following table describes the switch port default settings.

Table 5-1. Port Default Settings

Function	Default Setting
Port speed and mode	1000M Auto-negotiation
Port forwarding state	Enabled
Head of line blocking prevention	On (Enabled)
Flow Control	Off
Back Pressure	Off

The following is an example for changing the port speed on port g1 using CLI commands:

```
Console (config)# interface ethernet g1
Console (config-if)# speed 100
```

The following is an example for enabling flow control on port g1 using CLI commands:

```
Console (config)# interface ethernet g1
Console (config-if)# flowcontrol on
```

The following is an example for enabling back pressure on port g1 using CLI commands. Backpressure works only for the 10-Mbps mode of operation.

```
Console (config)# interface ethernet g1
Console (config-if)# speed 10
Console (config-if)# back-pressure
```

Terminal Connection Configuration

Your switch requires the following Terminal Connection parameters for configuration:

- no parity
- one stop bit
- 8 data bits

Baud Rate

The baud rates can be manually changed to any of the following values:

- 2400
- 4800
- 9600
- 19200
- 115,200

NOTE: The default baud rate is 115,200.

NOTE: Closing the device does not return the default baud rate. It must be specifically configured.

NOTE: The baud rate setting of the console is not saved in the general configuration file of the switch. It is directly stored in the non-volatile memory device of the switch.

The following is an example configuration for changing the default baud rate using CLI commands:

```
console# configure
console(config)# line console
console(config-line)# speed 115200
```

Other Configuration Requirements

The following is required for downloading embedded software and configuring the device:

- ASCII terminal (or emulation) connected to the serial port (cross-cable) in the front of the unit
- Assigned IP address for the switch for device remote control use with Telnet, SSH, and so forth

NOTE: The configuration process defines only one port.

Booting the Switch

When the power is turned on with the local terminal already connected, the switch goes through Power On Self Test (POST). POST runs every time the device is initialized and checks hardware components to determine if the device is fully operational before completely booting.

If a critical problem is detected, the program flow stops. If POST passes successfully, a valid executable image is loaded into RAM.

POST messages are displayed on the terminal and indicate test success or failure.

To boot the switch, perform the following steps:

1. Ensure that the ASCII cable is connected to the terminal.
2. Connect the power supply to the switch.
3. Power on the switch.

   As the switch boots, the bootup test first counts the device memory availability and then continues to boot. The following screen is an example of the displayed POST:

```
Boot1 Checksum Test.............................PASS
Boot2 Checksum Test.............................PASS
Flash Image Validation Test.....................PASS
Testing CPU PCI Bus Device Configuration.........PASS


 BOOT Version 1.0.0.13  Date  13-Aug-2003  Time  15:28:31


Autoboot in 2 seconds - press RETURN or Esc. to abort and enter
prom.
```

The boot process runs approximately 30 seconds.

The auto-boot message that appears at the end of POST (see the last lines) indicates that no problems were encountered during boot.

During boot, you can use the **Startup** menu, if necessary to run special procedures. To enter the **Startup** menu, press <Esc> or <Enter> within the first two seconds after the auto-boot message appears. For information on the **Startup** menu, see "Startup Menu Functions."

If you do not interrupt the system boot by pressing <Esc> or <Enter>, the system continues operation by decompressing and loading the code into RAM. The code starts running from RAM and the list of numbered system ports and their states (up or down) are displayed.

NOTE: TThe following screen is an example configuration. Items such as addresses, versions, and dates may differ for each device.

```
Preparing to decompress...


Decompressing SW from image-1

d04000

OK

Running from RAM...


********************************************************************
****

** Running  SW  Ver. 1.0.1.06  Date  15-Sep-2003  Time
17:48:07 **

********************************************************************
****


HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is  : 256M bytes

Dram first block size is  : 235520K bytes

Dram first PTR is  : 0x1800000

Dram second block size is  : 1984K bytes

Dram second PTR is  : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003
11:20:13
```

```
PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization
task is completed


Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed
- not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed
- operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status
changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status
changed - operational.

console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product
global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down:  g1

18-May-2003 16:24:42 %LINK-W-Down:  g2
```

After the switch boots successfully, a system prompt appears (`console>`) and you can use the local terminal to begin configuring the switch. However, before configuring the switch, ensure that the software version installed on the device is the latest version. If it is not the latest version, download and install the latest version. See "Software Download and Reboot."

Configuration Overview

Your switch supports a 10/100 Mbps Ethernet Out-of-Band (OOB) management port that is connected directly to the device. This port supports system-administrator management applications. The Out-of-Band port is treated as an IP interface to the system, and all management interfaces are available over this port. The Out-of-Band port does not support user traffic. Packets are not switched or routed from any in-band port (Ethernet port other than Out-of-Band) to the Out-of-Band port.

Before configuring the device, obtain the following information from the network administrator:

- IP address of the Out-of-Band port
- IP subnet mask for the network
- Default gateway (next hop router) IP address for configuring the default route

There are two types of configuration: Initial configuration consists of configuration functions with basic security considerations, whereas advanced configuration includes dynamic IP configuration and more advanced security considerations.

NOTICE: After making any configuration changes, the new configuration must be saved before rebooting. To save the configuration, enter:

```
console# copy running-config startup-config
```

Initial Configuration

The initial configuration can be done using the Setup Wizard or the CLI. The Setup Wizard is automatically entered when the device configuration file is empty. CLI can be invoked by entering [ctrl+z].

This guide shows how to use the Setup Wizard for initial device configuration. The Setup Wizard configures the following fields.

- SNMP Community String and SNMP Management System IP address (optional)
- Username and Password
- Device IP address
- Out-of-Band's default gateway address

After the device completes the POST and is booted, the following is displayed:

```
Welcome to Dell Easy Setup Wizard

The Setup Wizard guides you through the initial switch
configuration, and gets you up and running easily and quickly.
You can also skip the setup wizard, and enter CLI mode to
manually configure the switch if you prefer.

You can exit the Setup Wizard at any time by entering [ctrl+Z].
```

```
The system will prompt you with a default answer; by pressing
enter, you accept the default.

After you configure basic settings using the Setup Wizard, you
can manage the device from the Out-of-band management port.

Would you like to enter the setup wizard? [Y/N] Y
```

1 If [N] is entered, the Setup Wizard is exited. If there is no response within 60 seconds, the Setup Wizard is automatically exited and the CLI console prompt is displayed. If [Y] is entered, the Setup Wizard provides interactive guidance through the initial device configuration.

NOTE: If there is no response within 60 seconds, and there is a BootP server on the network, an address is retrieved from the BootP server.

NOTE: The user can exit the Setup Wizard at any time by entering [ctrl+z].

Wizard Step 1

If [Y] is entered the following is displayed:

```
The system is not setup for SNMP management by default. To
manage the switch using SNMP (required for Dell Network
Manager) you can:

• Setup the initial SNMP version 2 account now.
• Return later and setup the SNMP version 2 account. (For more
  information on setting up a SNMP version 2 account, see the
  user documentation).

Would you like to setup the SNMP management interface now?
  [Y/N] Y
```

2 Enter [N] to skip to Step 2 or enter [Y] to continue the Setup Wizard. If [Y] is entered the following is displayed:

```
To setup the SNMP management account you must specify the
management system IP address and the "community string" or
password that the particular management system uses to access
the switch. The wizard automatically assigns the highest access
level [Privilege Level 15] to this account. You can use Dell
Network Manager or other management interfaces to change this
setting later, and to add additional management system later.
For more information on adding management systems, see the user
documentation.

To add a management station:

Please enter the SNMP community string to be used:
```

```
Please enter the Management System IP address(A.B.C.D) or
wildcard (0.0.0.0) to manage from any Management Station:
```

3 Enter the following:
   – User SNMP community string, for example "MYSETUPWIZARD"
   – Management System IP address for example "0.0.0.0".

4 Press **Enter**.

Wizard Step 2

The following is displayed:

```
Now we need to setup your initial privilege (Level 15) user
account. This account is used to login to the CLI and Web
interface. You may setup other accounts and change privilege
levels later. For more information on setting up user accounts
and changing privilege levels, see the user documentation.

To setup a user account:

Please enter the user name:

Please enter the user password:

Please reenter the user password:
```

5 Enter the following:
   – User name, for example "admin"
   – Password and password confirmation.

NOTE: If the first and second password entries are not identical, the user is prompted until they are identical.

6 Press **Enter**.

Wizard Step 3

7 The following is displayed:

```
Next, an IP address is setup. The IP address is defined on the
OOB port. This is the IP address you use to access the CLI, Web
interface, or SNMP interface for the switch.

To setup an IP address:

Please enter the device IP address(A.B.C.D):

Please enter the IP subnet mask (A.B.C.D or /nn):
```

8 Enter the IP address and IP subnet mask, for example 192.168.1.100 as the IP address and 255.255.255.0 as the IP subnet mask.

NOTE: Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are invalid.

9 Press **Enter**.

Wizard Step 4

The following is displayed:

```
Finally, setup the default gateway. Please enter the gateway IP
address from which this network is reachable (e.g.
192.168.1.1):
```

10 Enter the default gateway.

11 Press **Enter**. The following is displayed (as per the example parameters described):

```
This is the configuration information that has been collected:

SNMP Interface = MYSETUPWIZARD@0.0.0.0

User Account setup = admin

Password = **********

Management IP address = 192.168.1.100 255.255.255.0

Default Gateway = 192.168.1.1
```

Wizard Step 5

The following is displayed:

```
If the information is correct, please select (Y) to save the
configuration, and copy to the start-up configuration file. If
the information is incorrect, select (N) to discard
configuration and restart the wizard: [Y/N]
```

12 Enter [N] to skip to restart the Setup Wizard or enter [Y] to complete the Setup Wizard. If [Y] is entered the following is displayed:

```
Configuring SNMP management interface.

Configuring user account.......

Configuring IP and subnet......

.............................

Thank you for using Dell Easy Setup Wizard. You will now enter
CLI mode.
```

Wizard Step 6

The CLI prompt is displayed.

The device can now be managed either from the already connected Console port or remotely through the Out-of-Band interface defined during the initial configuration.

Advanced Configuration

This section provides information about dynamic allocation of IP addresses and security management based on the authentication, authorization, and accounting (AAA) mechanism.

When configuring/receiving IP addresses through DHCP and BOOTP, the configuration received from these servers includes the IP address, and may include subnet mask and default gateway.

Retrieving an IP Address From a DHCP Server

When using the DHCP protocol to retrieve an IP address, the device acts as a DHCP client.

To retrieve an IP address from a DHCP server, perform the following steps:

1. Select and connect any port to a DHCP server or to a subnet that has a DHCP server on it, in order to retrieve the IP address.
2. Enter the following commands to use the selected port for receiving the IP address. In the following example, the commands are based on the port type used for configuration.
   - Assigning Dynamic IP Addresses (on an InBand Port):

```
console# configure
console(config)# interface ethernet g1
console(config-if)# ip address dhcp hostname <string>
console(config-if)# exit
```

   - Assigning Dynamic IP Addresses (on an Out-of-Band Port)

```
console# configure
console(config)# interface out-of-band-eth
console(config-oob)# ip address dhcp hostname dell
console(config-oob)# exit
console(config)# exit
```

   The interface receives the IP address automatically.

3. To verify the IP address, enter the **show ip interface** command at the system prompt as shown in the following example.

```
console# show ip interface
IP Address       I/F         Type      Directed Broadcast
---------------------- --------------------- --------------
```

```
100.1.1.1/24    vlan 1      static       disable

OOB ip interfaces

Gateway IP Address      Activity status
----------------------- -----------------------
10.6.12.1               active

IP Address     I/F                    Type
-------------- ---------------------- ---------
10.6.12.20/24 Oob-eth 1               dhcp
```

NOTE: You do not need to delete the device configuration to retrieve an IP address for the DHCP server.

NOTE: TWhen copying configuration files, avoid using a configuration file that contains an instruction to enable DHCP on an interface that connects to the same DHCP server, or to one with an identical configuration. In this instance, the switch retrieves the new configuration file and boots from it. The switch then enables DHCP as instructed in the new configuration file, and the DHCP instructs it to reload the same file again.

Receiving an IP Address From a BOOTP Server

The standard BOOTP protocol is supported and enables the switch to automatically download its IP host configuration from any standard BOOTP server in the network. In this case, the device acts as a BOOTP client.

To retrieve an IP address from a BOOTP server:

1. Select and connect any port to a BOOTP server or subnet containing such a server, to retrieve the IP address.
2. At the system prompt, enter the **delete startup configuration** command to delete the startup configuration from flash.

   The device reboots with no configuration and in 60 seconds starts sending BOOTP requests.

   The device receives the IP address automatically.

NOTE: When the device reboot begins, any input at the ASCII terminal or keyboard automatically cancels the BOOTP process before completion and the device does not recieve an IP address from the BOOTP server.

The following example illustrates the process:

```
console> enable
```

```
console# delete startup-config
Startup file was deleted
console# reload
You haven't saved your changes. Are you sure you want to
continue (y/n) [n]?
This command will reset the whole system and disconnect your
current session. Do you want to continue (y/n) [n]?
*****************************************************
/* the device reboots */
```

To verify the IP address, enter the **show ip interface** command.

The device is now configured with an IP address.

Security Management and Password Configuration

System security is handled through the AAA (Authentication, Authorization, and Accounting) mechanism that manages user access rights, privileges, and management methods. AAA uses both local and remote user databases. Data encryption is handled through the SSH mechanism.

The system is delivered with no default password configured; all passwords are user-defined. If a user-defined password is lost, a password recovery procedure can be invoked from the **Startup** menu. The procedure is applicable for the local terminal only and allows a one-time access to the device from the local terminal with no password entered.

Configuring Security Passwords

The security passwords can be configured for the following services:

- Console
- Telnet
- SSH
- HTTP
- HTTPS

NOTE: Passwords are user-defined.

NOTE: YWhen creating a user name, the default priority is "1," which allows access but not configuration rights. A priority of "15" must be set to enable access and configuration rights to the device. Although user names can be assigned privilege level 15 without a password, it is recommended to always assign a password. If there is no specified password, privileged users can access the Web interface with any password

Configuring an Initial Console Password

To configure an initial console password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password george
```

- When initially logging on to a device through a console session, enter **george** at the password prompt.
- When changing a device's mode to enable, enter **george** at the password prompt.

Configuring an Initial Telnet Password

To configure an initial Telnet password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
```

- When initially logging onto a device through a Telnet session, enter `bob` at the password prompt.
- When changing a device mode to enable, enter `bob`.

Configuring an Initial SSH password

To configure an initial SSH password, enter the following commands:

```
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password jones.
```

- When initially logging onto a device through a SSH session, enter `jones` at the password prompt.
- When changing a device's mode to enable, enter `jones`.

Configuring an Initial HTTP Password

To configure an initial HTTP password, enter the following commands:

```
console(config)# ip http authentication local
console(config)# username admin password user1 level 15
```

Configuring an initial HTTPS password:

To configure an initial HTTPS password, enter the following commands:

```
console(config)# ip https authentication local
console(config)# username admin password user1 level 15
```

NOTE: You should generate a new crypto certificate each time you upgrade (install a new version of) the control software application on the device.

Enter the following commands once when configuring to use a console, a Telnet, or an SSH session in order to use an HTTPS session.

In the Web browser enable SSL 2.0 or greater for the page content to appear.

```
console(config)# crypto certificate generate key_generate
console(config)# ip https server
```

When initially enabling an http or https session, enter `admin` for user name and `user1` for password.

NOTE: Http and Https services require level 15 access and connect directly to the configuration level access.

Software Download and Reboot

Software Download Through XModem

This section contains instructions for downloading device software (system and boot images) using XModem, which is a data transfer protocol for updating back-up configuration files.

To download a boot file using XModem:

1. Enter the command **console# xmodem: boot**.

   The switch is ready to receive the file via the XModem protocol and displays text similar to the following:

   ```
   console# copy xmodem: boot
   ```

```
Please download program using XMODEM.
console#
```

2. Specify the source file path within 20 seconds.

   If the path is not specified within 20 seconds, the command times out.

To download a software image file using XModem:

1. Enter the command **console# xmodem: image**.

   The switch is ready to receive the file via the XModem protocol.

2. Specify the source file path to begin the transfer process.

   The following is an example of the information that appears:

```
console# copy xmodem: image
Please download program using XMODEM.
console#
```

Software Download Through TFTP Server

This section contains instructions for downloading switch software (system and boot images) through a TFTP server. The TFTP server must be configured before downloading the software.

The switch boots and runs when decompressing the system image from the flash memory area where a copy of the system image is stored. When a new image is downloaded, it is saved in the other area allocated for the additional system image copy.

On the next boot, the switch decompresses and runs the currently active system image unless chosen otherwise.

To download an image through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Make sure that the file to be downloaded is saved on the TFTP server (the DOS file).
3. Enter the command **console# show version** to verify which software version is currently running on the device.

   The following is an example of the information that appears:

```
console# show version
SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
HW version
```

4. Enter the command **console# show bootvar** to verify which system image is currently active. The following is an example of the information that appears:

```
console# show bootvar
Images currently available on the Flash
Image-1 active (selected for next boot)
Image-2 not active
console#
```

5 Enter the command **console# copy tftp://{tftp address}/{file name} image** to copy a new system image to the device.

When the new image is downloaded, it is saved in the area allocated for the other copy of system image (image-2, as given in the example). The following is an example of the information that appears:

```
console# copy tftp://176.215.31.3/file1 image
Accessing file file1 on 176.215.31.3...

Loading file1 from 176.215.31.3:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!! Copy took 00:01:11 [hh:mm:ss]
```

Exclamation symbols indicate that a copying process is in progress. A period indicates that the copying process is timed out. Many periods in a row indicate that the copying process failed.

6 Select the image for the next boot by entering the **boot** system command. After this command, enter the command **console# show bootvar** to verify that the copy indicated as a parameter in the boot system command is selected for the next boot.

The following is an example of the information that appears:

```
console# boot system image-2
console# sh bootvar
Images currently available on the Flash
Image-1 active
Image-2 not active (selected for next boot)
```

If the image for the next boot is not selected by entering the boot system command, the system boots from the currently active image (image-1, as given in the example).

7 Enter the command **reload**. The following message is displayed:

```
console# reload
This command will reset the whole system and disconnect your
current session. Do you want to continue (y/n) [n] ?
```

8 Enter **Y** to reboot the switch.

Boot Image Download

Loading a new boot image from the TFTP server and programming it into the flash updates the boot image. The boot image is loaded when the switch is powered on.

To download a boot file through the TFTP server:

1. Ensure that an IP address is configured on one of the device ports and pings can be sent to a TFTP server.
2. Make sure that the file to be downloaded (the **.rfb** file) is saved on the TFTP server.
3. Enter the command **console# show version** to verify which boot version is currently running on the device.

   The following is an example of the information that appears:

   ```
   console# show version
   SW version 3.31.42 ( date 22-Jul-2003 time 13:42:41 )
   Boot version 1.31.03 (date 01-Jun-2003 time 15:12:20 )
   HW version 00.00.01 (date 01-May-2003 time 12:12:20 )
   ```

4. Enter the command **console# copy tftp://{tftp address}/{file name} boot** to copy the boot image to the switch.

   The following is an example of the information that appears:

   ```
   console# copy tftp://176.215.31.3/6024_boot-10013.rfb
   Erasing file ...done.
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
   !!!!!!!! Copy: 393232 bytes copied in 00:00:05 [hh:mm:ss]
   ```

5. Enter the command **reload**.

   The following message is displayed:

   ```
   console# reload
   This command will reset the whole system and disconnect your
   current session. Do you want to continue (y/n) [n] ?
   ```

6. Enter **Y** to reboot the switch.

Sample Configuration Process

This section provides the basic steps required to establish a remote network management connection with the switch. This section does not explain the various configurations available on the switch or the relevant commands.

This section also describes accessing a switch for the first time with the default configuration and definitions. If a previously entered configuration causes problems, the startup-configuration file—which is the configuration of device when powered up—should be erased and device rebooted, see "Device Default Settings."

Device Setup Requirements

The following components are required for the purpose of this example:

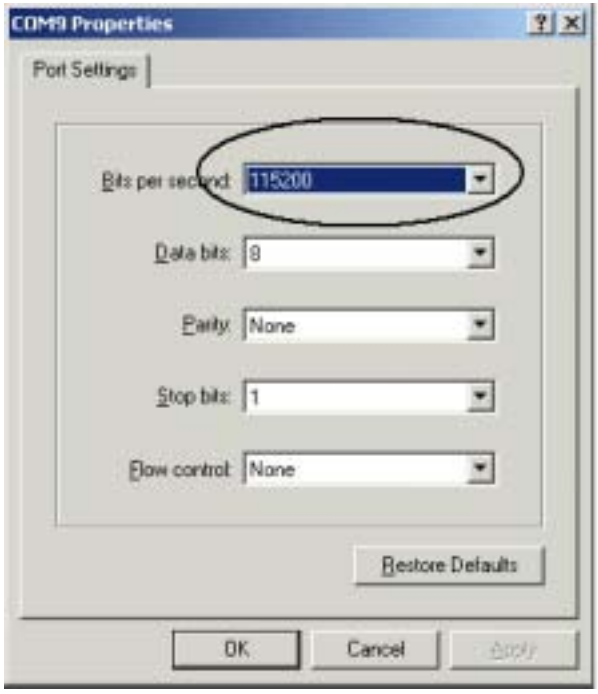
- PowerConnect 6024/6024F switch
- A workstation with the following components installed:
  - Network adapter card
  - ASCII terminal application (for example, Microsoft® Windows® HyperTerminal or Procomm Plus Terminal)
  - A browser application
- One Null Modem F2F cable.
- Straight or cross UTP (category 5) cable(s)

Initial Connection

1. Using the RS-232 port, connect the switch to the workstation.
2. Set the ASCII terminal with the following settings and select the appropriate COM port.

   The sample screen uses the HyperTerminal.

Figure 5-2. HyperTerminal Properties Window



NOTE: 115,200 is the default baud rate for new device. The device may have another baud rate. If using the 115,200 baud rate does not result in viewing the device terminal, try other baud rate.

3 Use an F2F null modem cable to connect the workstation to the switch.

4 Connect the device power cord and power up the device.

The following screen is displayed:

```
************************************************
*****************  SYSTEM RESET  *****************
************************************************


Booting...


Boot1 Checksum Test.............................PASS
Boot2 Checksum Test.............................PASS
Flash Image Validation Test.....................PASS
```

```
Testing CPU PCI Bus Configuration.................PASS


 BOOT Version 1.0.0.13  Date  13-Aug-2003  Time  15:28:31


Autoboot in 2 seconds - press RETURN or Esc. to abort and enter
prom.
```

At this point, you can enter the **Startup** menu, if necessary, to run special procedures. If you do not enter the **Startup** menu, the system continues operation by decompressing the code into RAM. The code starts running from RAM and the list of available port numbers and their states (up or down) are displayed.

NOTE: The following screen is an example configuration. Items such as addresses, versions, and dates may differ for each device.

```
Preparing to decompress...


Decompressing SW from image-1

d04000

OK

Running from RAM...


**************************************************************
*******

*** Running  SW  Ver. 1.0.1.06  Date  15-Sep-2003  Time
17:48:07 ***

**************************************************************
*******


HW version is 00.01.64

Base Mac address is: 00:00:b0:16:00:00

Dram size is  : 256M bytes

Dram first block size is  : 235520K bytes

Dram first PTR is  : 0x1800000

Dram second block size is  : 1984K bytes
```

```
Dram second PTR is  : 0xFE00000

Flash size is: 16M

Tuning File info. Ver: 0.2.80 Creation date: Aug 20 2003
11:20:13

PowerConnect 6024

Tapi Version: v1.1a1-P18

Core Version: v1.1a1-P18

18-May-2003 16:24:41 %INIT-I-InitCompleted: Initialization
task is completed




Start the sync process between devices 0 - 1


Sync OK


18-May-2003 16:24:41 %Box-W-PS-STAT-CHNG: PS# 1 status changed
- not operational

.

18-May-2003 16:24:41 %Box-I-PS-STAT-CHNG: PS# 2 status changed
- operational.

18-May-2003 16:24:41 %Box-W-FAN-STAT-CHNG: FAN# 1 status
changed - operational.

18-May-2003 16:24:41 %Box-I-FAN-STAT-CHNG: FAN# 2 status
changed - operational.

console> 18-May-2003 16:24:41 %DELL-I-STATUS: The product
global status has chan

ged from ok to non-critical at time 900.

18-May-2003 16:24:42 %LINK-W-Down:  g1

18-May-2003 16:24:42 %LINK-W-Down:  g2
```

```
The device is ready for configuration.
```

Device Default Settings

To return to device default settings use **delete startup-config** command at the privileged mode prompt (#), and reboot the device. Once device reloads – it is set with the default settings.

```
console>

console> enable

console# delete startup-config

Startup file was deleted

console# reload

This command will reset the whole system and disconnect your
current

session. Do you want to continue (y/n) [n] ?

y


************************************************

*****************  SYSTEM RESET  *****************

************************************************

.

.

.

.
```

Enabling Remote Management

1. Enter the **enable** command at the console to enter the Privileged EXEC screen mode as follows:

   ```
   console>enable

   console#
   ```

2. Connect the management station (PC) to the device via one of the Ethernet ports, or through a network connected to the device, using a CAT5 Cable.

This example will use port g1.

3 Ensure (on the ASCII terminal) that the interface status changed to "up" and that the STP status is forwarding (after 30 seconds) as shown below:

```
Console#

01-Jan-2000 01:43:03 %LINK-I-Up:  Vlan 1

01-Jan-2000 01:43:03 %LINK-I-Up:  g1

01-Jan-2000 01:43:34 %STP-I-PORTSTATUS: Port g1: STP status
Forwarding
```

4 Enter the **config** command at the console to enter the Configuration screen mode as follows:

```
console# config
```

5 Enter the **interface vlan** command at the console to enter the VLAN Configuration screen mode through the default VLAN 1 (tag = 1) as follows:

```
console(config)# interface vlan 1

console (config-if)#
```

6 Define an IP address on the device by assigning an IP address (in this example 50.1.1.1) to the VLAN containing the interface connected to the management station . If the management station is connected directly to the interface, the IP address on the VLAN must have the same subnet as the management station.

```
console(config)#

console(config-if)# ip address 50.1.1.1 225.0.0.0

console(config-if)#
```

7 If the management station is a member of a remote network, and is not directly connected to the interface, configure a static route.

The configured IP address must belong to the same subnet as one of the device IP interfaces. In this example the static address is 50.1.1.100.

```
console(config-if)# exit

console(config)# ip route 0.0.0.0.0.0.0.0 50.1.1.100

console(config)#
```

8 Ping the management station from the switch to make sure that connectivity has been achieved.

Wait 30 seconds for port to be in STP forwarding before pinging the management station. Management station IP is (in this example) 50.1.1.2:

```
console(config)#
```

```
console(config)# exit
console# ping 50.1.1.2
64 bytes from 50.1.1.2: icmp_seq=1. time=0 ms
64 bytes from 50.1.1.2: icmp_seq=2. time=0 ms
64 bytes from 50.1.1.2: icmp_seq=3. time=0 ms
64 bytes from 50.1.1.2: icmp_seq=4. time=0 ms

----50.1.1.2 PING Statistics----
4 packets transmitted, 4 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
console#
```

9 Define a user name and password to allow privileged level 15 device access for a remote user (HTTP and HTTPS).

In this example the user name and password is "Dell," user name is "Dell," and the privilege level is 15. Privilege levels range from 1-15, with 15 being the highest level. Level 15 access is the only level of access for the Web interface.

```
console# config
console(config)# username Dell password Dell privilege 15
console(config)# ip http authentication local
console(config)# ip https authentication local
console(config)# crypto certificate generate key_generate
Generating RSA private key, 1024 bit long modulus
console(config)# ip https server
```

10 Define a user name and password to allow access for a local user—console, Telnet, Web Server, for example.

In this example the user name and password is "Dell," and the privilege level is 15.

```
console(config)# username Dell password Dell privilege 15
console(config)#
console(config)# aaa authentication login default line
console(config)# aaa authentication enable default line
console(config)# line console
```

```
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password tom
console(config-line)# exit
console(config)# line telnet
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password bob
console(config-line)# exit
console(config)# line ssh
console(config-line)# login authentication default
console(config-line)# enable authentication default
console(config-line)# password jones
console(config-line)# exit
```

11 Save the **running-config** file to the **startup-config** file.

This ensures that the configuration just completed is the same if the device is rebooted.

```
console(config-line)# exit
console(config)# exit
console# copy running-config startup-config
```

The device is now configured and can be managed through the different options such as Telnet, Web browser interface, and others.

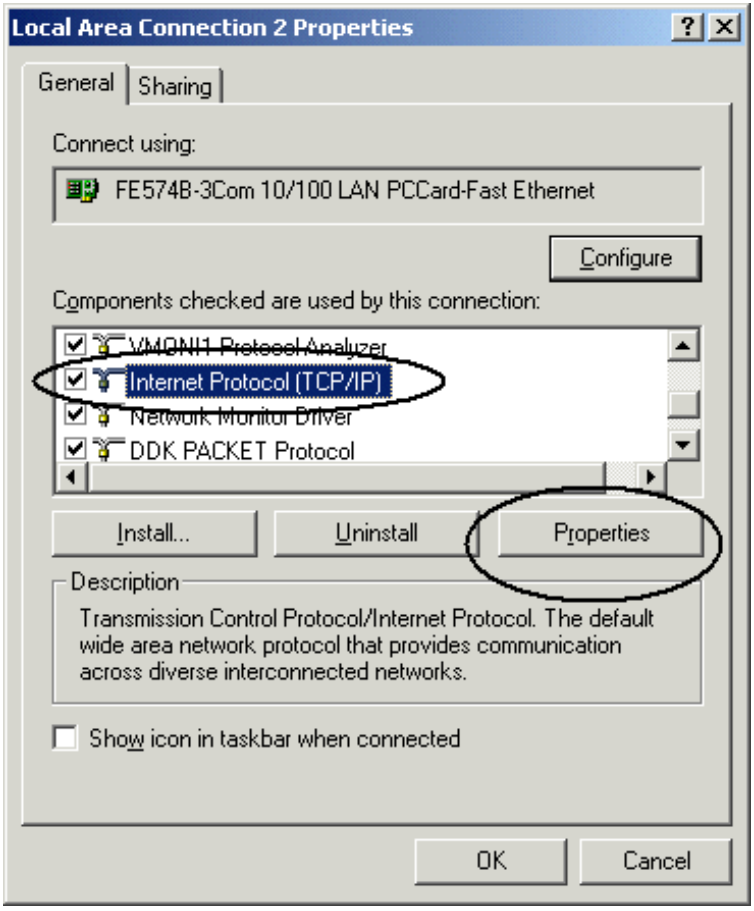
Setting the Management Station IP Address

1 On the management station, click **Start→Settings→Network and Dial-up Connections**.

2 Right-click the network connection that is used for management, and select **Properties**.

The connection properties window is displayed.

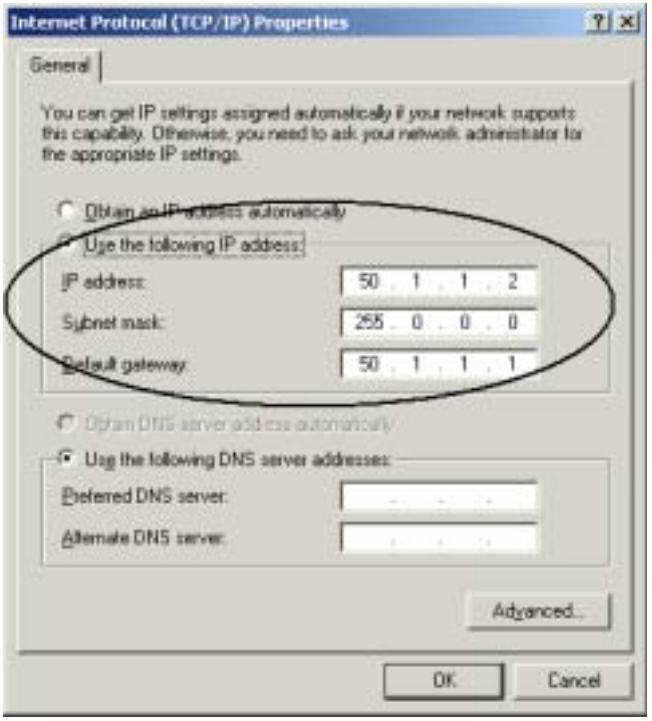
Figure 5-3. Local Area Connection Properties Window



3 Click **Internet Protocol (TCP/IP)** and then click **Properties**.

The **Internet Protocol (TCP/IP) Properties** window is displayed.

Figure 5-4. Internet Protocol (TCP/IP) Properties Window



4 Click **Use the following IP address**.

5 Enter the appropriate addresses for the management station in the **IP address**, **Subnet mask**, and **Default gateway** fields.

NOTE: If the management station is connected to a router and not directly to the 6024/6024F switch, the default gateway must be configured as the router interface IP address connected to the management station (which leads to the 6024/6024F switch).

Enabling Telnet Access

Use the Windows/DOS command line or a Telnet application to access the device via a Telnet. Remember to enter the appropriate password. The connection is done with the IP address defined on the device.

When access is granted, command usage is the same as in direct device management:

1 On the management station, click **Start→Run.**

2 In the **Run** window, type `cmd` and click **OK**.

The standard Windows command line interface is displayed.

3 Enter the command **Telnet** and the device IP address, such as the following:

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>telnet 50.1.1.1
11-Aug-20 03 11:14:06 %MSCM-I-NEWTERM: New TELNET connection
from 50.1.1.2
Password:***
console> enable
Password:***
console# show ip interface
Proxy ARP is disabled
IP Address    I/F      Type   Directed Broadcast
------------ -------  ------ ---------------
100.1.1.1/24  vlan 1 static disable

OOB ip interfaces
Gateway IP Address      Activity status
----------------------- -----------------------
10.6.12.1               active

IP Address                 I/F                  Type
---------------------- ---------------------- ---------
10.6.12.20/24          Oob-eth 1              dhcp
```

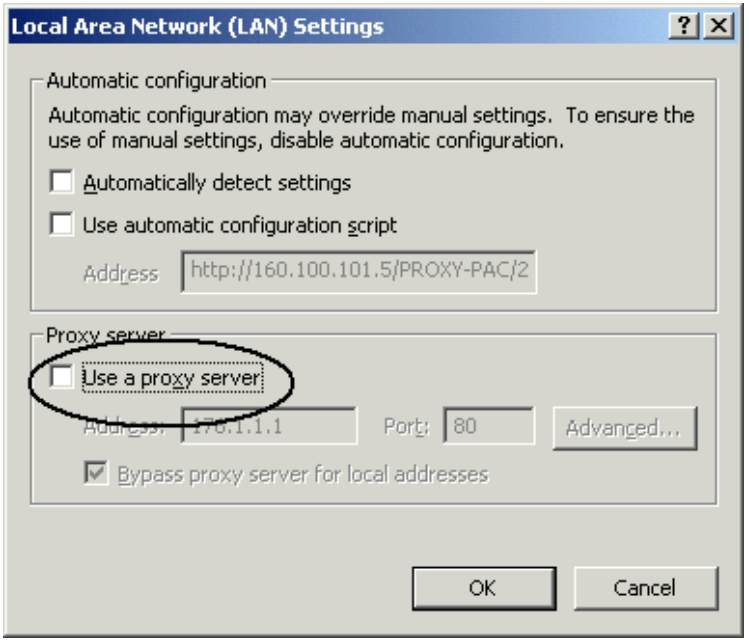
The switch indicates the Telnet session status:

```
console> 01-Jan-2000 02:39:04 %MSCM-I-NEWTERM: New TELNET
connection from 50.1.1.2
01Jan-2000 02:39:11 %MSCM-I-TERMTERMINATED: TELNET connection
from 50.1.1.2 terminated
```

Enabling Web Access (HTTP Server)

1. To prevent problems that may occur when using an HTTP proxy server, disable (uncheck) the proxy setting on the browser.
   a. In Microsoft Internet Explorer, click **Tools→Internet Options**.
   b. Click the **Connections** tab and then click **LAN Settings** to display the **Local Area Network (LAN) Settings** window.
   c. Ensure that the **Use a proxy server** check box is cleared, and then click **OK**.

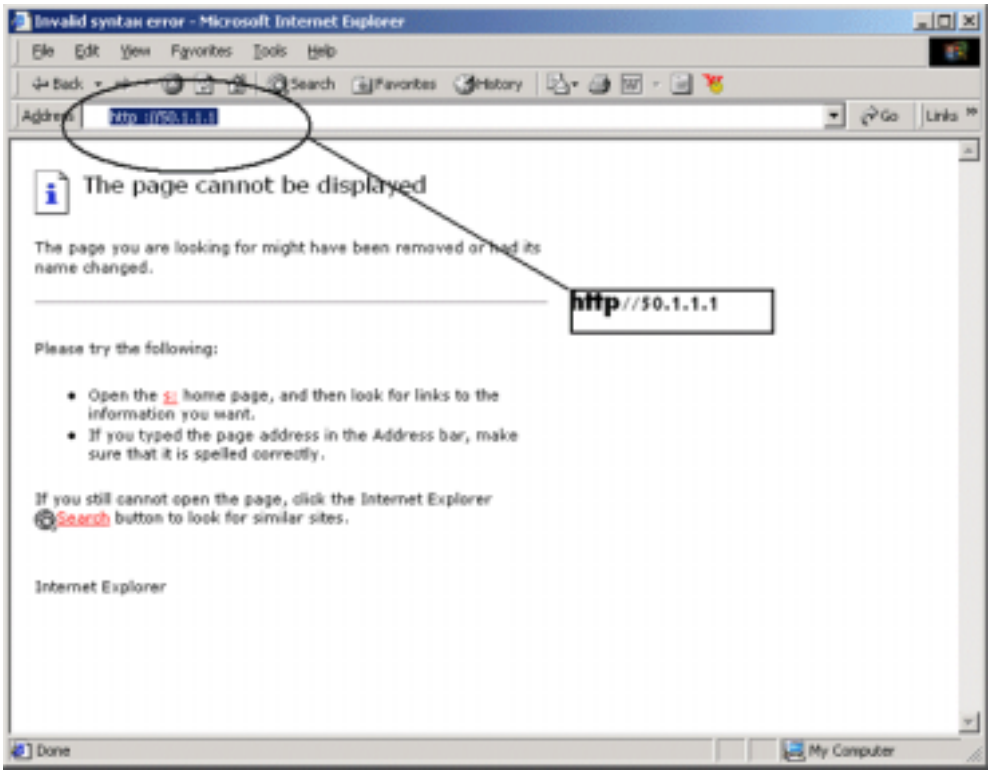
Figure 5-5. Local Area Network (LAN) Settings Window



   d. Click **OK** to close the **Internet Options** window.

2. In the browser window enter the IP previously configured on the device (with or without http:// prefix).

Figure 5-6. Logging onto the Web Interface



The password authentication window is displayed.

3 Enter the assigned user name and password.

The Dell OpenManage Switch Administrator is displayed.

NOTE: If no password is defined, any password is accepted.

Figure 5-7. Dell OpenManage Switch Administrator Page

Configuring Secure Management Access (HTTPS)

When managing the device securely via the standard Web browser the SSL (Secure Socket Layer) security protocol is used.

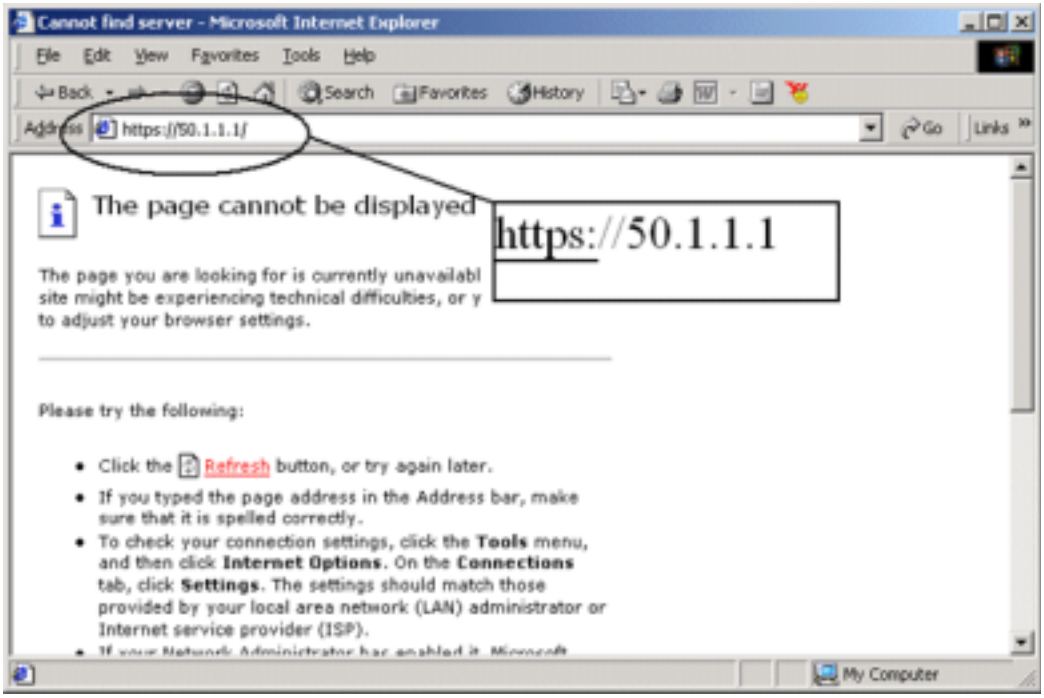
To manage the device securely via the standard Web browser, perform the following:

1. Configure the switch to allow HTTPS server, and to create a security key, use the commands **ip https server** and **crypto certificate generate key-generate**:

```
console# configure

console(config)# ip https server

console(config)# crypto certificate generate key-generate

Generating RSA private key, 1024 bit long modulus

console(config)#
```

2. Configure the management station the same as for a regular HTTP connection (see "Enabling Web Access (HTTP Server))".
3. Connect to the device via HTTPS by typing the address `https://<device IP address>` in the browser window (https must be typed):

Figure 5-8. Logging Onto the Web Interface With a Secure Connection



The **Security Alert** window is displayed.

4 Click **Yes** to confirm accept the security certification (if it is not authenticated by a third party).

5 The **Enter Network Password** window is displayed.

6 Enter the assigned user name and password.

The device Dell OpenManage Switch Administrator is displayed.

Startup Menu Functions

You can perform additional configuration from the **Startup** menu.

To display the **Startup** menu:

1 During the boot process, after the first part of the POST is completed press <Esc> or <Enter> within two seconds after the following message is displayed:

```
Autoboot in 2 seconds -press RETURN or Esc.to abort and enter
prom.
```

The **Startup** menu is displayed and contains the following configuration functions:

```
[1] Download Software
[2] Erase Flash File
[3] Erase Flash Sectors
[4] Password Recovery Procedure
[5] Enter Diagnostic Mode
[6] Back Enter your choice or press 'ESC' to exit:
```

The following sections describe the **Startup** menu options. If no selection is made within 25 seconds (default), the switch times out.

Only technical support personnel can operate the Diagnostics Mode. For this reason, the **Enter Diagnostic Mode** option of the **Startup** menu is not described in this guide.

Download Software

Use the software download option when a new software version must be downloaded to replace corrupted files, update, or upgrade the system software.

To download software from the **Startup** menu:

1. On the **Startup** menu, press <1>.

   The following prompt is displayed:

   ```
   Downloading code using XMODEM
   ```

2. When using HyperTerminal, click **Transfer** on the **HyperTerminal** menu bar.
3. From the **Transfer** menu, click **Send File**.

   The **Send File** window is displayed.

4. Enter the file path for the file to be downloaded.
5. Ensure the protocol is defined as Xmodem.
6. Click **Send**.

   The software is downloaded. Software downloading takes several minutes. The terminal emulation application, such as HyperTerminal, may display the loading process progress.

   After software downloads, the device reboots automatically.

Erase FLASH File

In some cases, the device configuration must be erased. If the configuration is erased, all parameters configured via CLI, Web browser interface, or SNMP must be reconfigured.

To erase the device configuration:

1. From the **Startup** menu, press <2> within 6 seconds to erase flash file.

   The following message is displayed:

   ```
   Warning! About to erase a Flash file.

   Are you sure (Y/N)? y
   ```

2. Press <Y>.

   NOTE: Do not press <Enter>.

   The following message is displayed.

   ```
   Write Flash file name (Up to 8 characters, Enter for
   none.):config File config (if present) will be erased after
   system initialization

   ======== Press Enter To Continue ========
   ```

3. Enter **config** as the flash file name.

   The configuration is erased and the device reboots.

4. Perform the switch's initial configuration.

Erase FLASH Sectors

For troubleshooting purposes, you may need to erase flash sectors. If the flash is erased, all software files must be downloaded and installed again.

To erase the FLASH:

1. From the **Startup** menu, press <3> within 6 seconds.

   The following message is displayed:

   ```
   Warning! About to erase Flash Memory! FLASH size = 16252928.
   blocks = 64 Are you sure (Y/N)
   ```

2. Confirm by pressing <Y>.

   The following message is displayed:

   ```
   Enter First flash block (1 - 63):
   ```

3. Enter the first flash block to be erased and press <Enter>.

   The value range is 1-64. The following message is displayed:

   ```
   Enter Last flash block (1 - 63):
   ```

4. Enter the last flash block to be erased and press <Enter>.
5. The following message is displayed:

   ```
   Are you sure (Y/N)
   ```

6 Confirm by pressing <Y>.

The following message is displayed:

```
Erasing flash blocks 1 - 63: Done.
```

Password Recovery

If a password is lost, use the **Password Recovery** option on the **Startup** menu. The procedure enables the user to enter the device once without a password.

To recover a lost password for the local terminal only:

1 From the **Startup** menu, select [4] and press <Enter>.

The password is deleted.

2 To ensure device security, reconfigure passwords for applicable management methods.

Out-of-Band Management Port

The Out-of-Band (OOB)management port is a 10/100-Mbps Ethernet port that can be used to connect directly to the switch to perform system administrator management functions. This port is regarded as a regular IP interface to the system, and all management interfaces are

available over this port.

No inband interfaces can be accessed via the Out-of-Band port. Similarly, the Out-of-Band port cannot be accessed via the inband ports. Because network management functionality can be performed using Out-of-Band, you should use the Out-of-Band port for all network management functions, including Web management; image, boot, and configuration download/upload; Telnet; SNMP management; and so forth.

Unlike the inband ports, Out-of-Band is not used for routing or switching purposes. Using the Out-of-Band port rather than an inband port for network management ensures that an additional inband (1- Gbyte) port remains active for routing.

The following sections contain examples of Out-of-Band commands.

Assigning Dynamic IP Addresses (on an Out-of-Band Port)

```
console#configure
console(config)#interface out-of-band-eth
console(config-oob)#ip address dhcp hostname dell
console(config-oob)#exit
console(config)#exit
console#
```

Assigning Static IP Addresses (on an Out-of-Band Port)

```
console>enable
console#configure
console(config)#interface out-of-band-eth
console(config-oob)#ip address 10.1.1.1 255.0.0.0
console(config-oob)#exit
console(config)#ip default-gateway 10.1.1.10
console(config)#exit
console#
```

Assigning IP Default Gateway

```
console>
console>enable
console#configure
console(config)#interface out-of-band-eth
console(config-oob)#ip address 10.0.0.1 /8
console(config-oob)#ip default-gateway 10.1.1.1
console(config-oob)#
```

Ping via Out-of-Band

```
console#ping oob/10.6.12.25
```

Copy Image/Boot

```
copy tftp://oob/10.6.12.25/ves_115.dos image
copy tftp://oob/10.6.12.25/boot_013.rfb boot
```

IP Default Gateway to Out-of-Band

```
console#configure
console(config)#interface out-of-band-eth
console(config-oob)#ip default-gateway 10.1.1.10
```

Additional Information

For more information about configuring Out-of-Band, see "Configuring Out-of-Band (OOB) Management Ports."

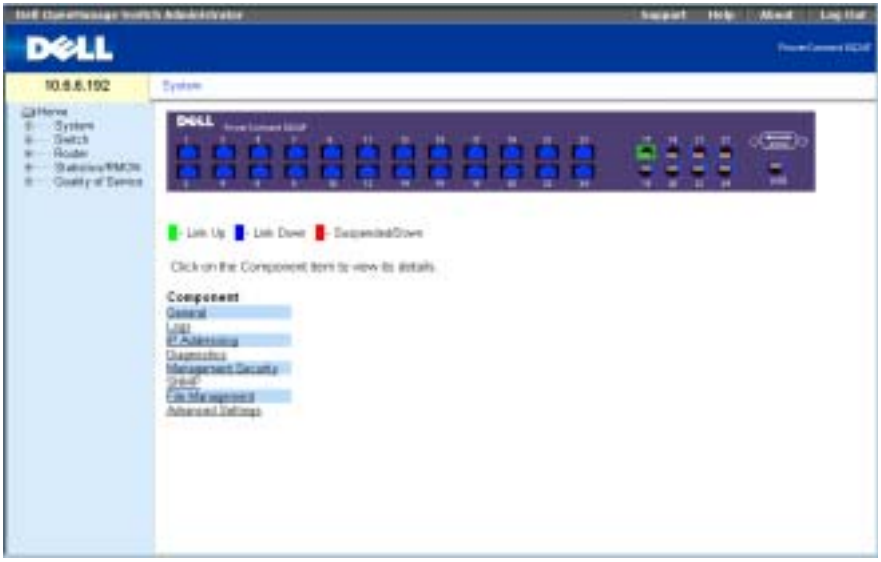
6

Configuring System Information

Opening the System Page

To open the **System** page, click **System** in the tree view (see Figure 6-1).

Figure 6-1. System



Defining General Device Information

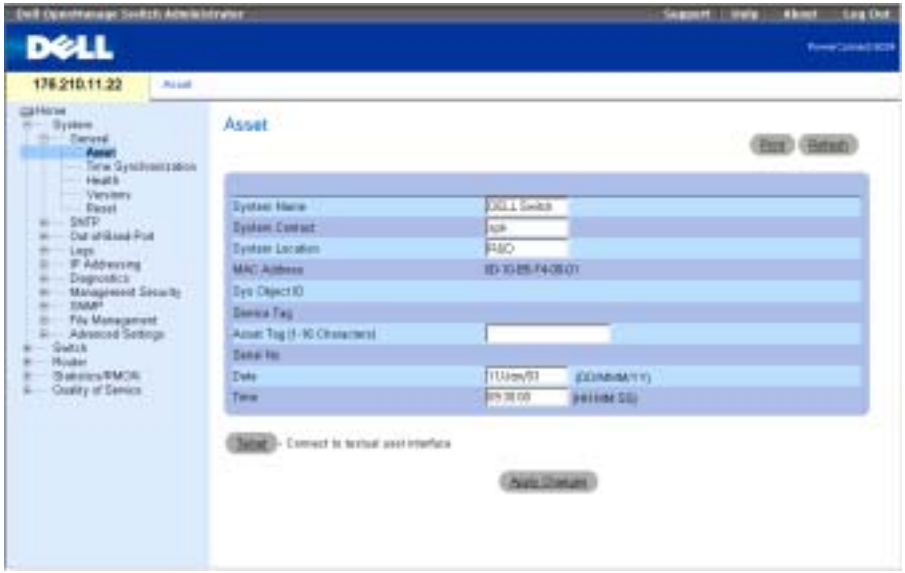
The **General** page contains links to pages that allow network managers to configure device parameters.

Configuring Device Information

The **Asset** page contains parameters for configuring and viewing general device information, including the system name, location, and contact, the system MAC address for both the switch and the out-of-band management port, system object ID, date, time, and system uptime.

To display the **Asset** page, click **System→General→Asset** in the tree view.

Figure 6-2. Asset



The **Asset** page contains the following fields:

System Name — The user-assigned device system nam.

System Contact —The contact person name.

System Location —The system runninglocation.

MAC Address —The MAC address switch .

Sys Object ID —The MIB OID.

Service Tag —The service reference number used when servicing the device.

Asset Tag —The user-defined device reference. The possible parameter values are 1 to 16.

Serial No.—The device serial number.

Date (DD/MMM/YY)—The current system date. The format is day, month, year, for example, 11/Jan/02 is January 11, 2002.

Time (HH/MM/SS)—The current system time. The format is hour, minute, second, for example, 20:12:03 is 8:12:03 PM.

Defining System Information

1. Open the **Asset** page.
2. Define the following fields: **System Name**, **System Contact**, **System Location**, and **Asset Tag**.
3. Click **Apply Changes**.

   The system parameters are applied, and the device is updated.

Initiating a Telnet Session

1. Open the **Asset** page.

NOTE: The appropriate telnet parameters are set prior to initiating the telnet session. See "Configuring an Initial Telnet Password" for information.

2. Click **Telnet**.

Configuring Device Information Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed in the **Asset** page.

Table 6-1. Asset CLI Commands

CLI Command	Description
`hostname name`	Specifies or modifies the device host name.
`snmp-server contact text`	Sets up a system contact.
`snmp-server location text`	Specifies information about where the device is located.
`show clock`	Displays the time and date from the system clock.
`asset-tag tag`	Specifies the asset tag for the device.
`show system-id`	Displays the system ID information, including service tag, asset tag, and serial number.
`show system`	Displays system information.

The following is an example of the CLI commands:

```
Console (config)# hostname dell
Console (config)# snmp-server contact Dell_Tech_Supp
Console (config)# snmp-server location New_Yorks
Console (config)# exit
Console# clock set 13:32:00 7 Mar 2002
Console# show clock
15:29:03 Jun 17 2002
```

Defining System Time Settings

The **Time Synchronization** page contains fields for synchronizing the system time with the local hardware clock or an external SNTP clock.

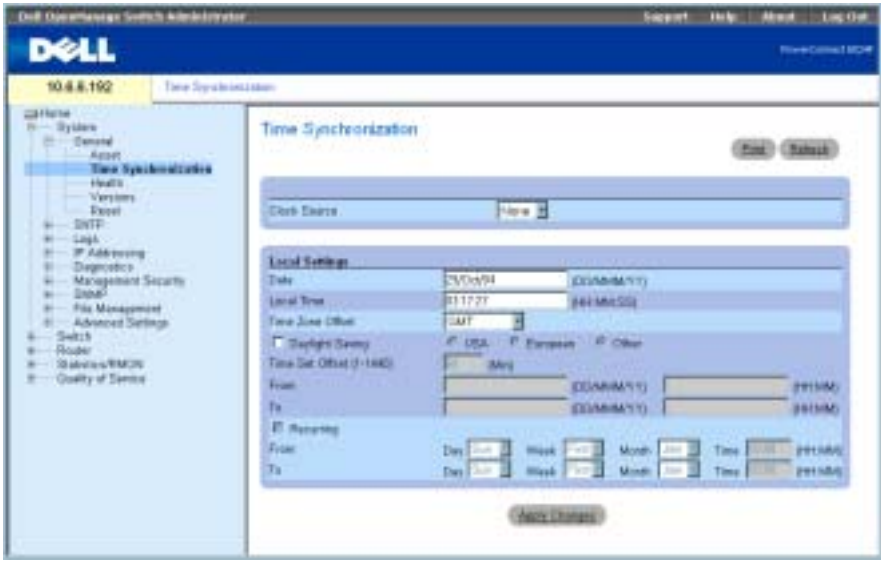
If the system clock is synchronized with an external SNTP clock and that clock fails, the system clock time source automatically switches to the local hardware clock.

The system clock can be configured to automatically switch to Daylight Savings Time.

For more information on SNTP, see **Configuring SNTP Settings**.

To open the **Time Synchronization** page, click **System →General →Time Synchronization** in the tree view.

Figure 6-3. Time Synchronization



The **Time Synchronization** page contains the following fields:

Clock Source — The time source used to maintain the system clock. The possible field values are:

None — Specifies that the system time is synchronized with the local hardware clock.

SNTP — Specifies that the system time is synchronized with an SNTP server clock. For more information, see **"Configuring SNTP Settings" on page 110**.

Date — Defines the system date. The field format is DD:MMM:YY.

Local Time — Defines the system time. The field format is HH:MM:SS.

Time Zone Offset — Defines the difference in hours between Greenwich Mean Time (GMT) and local time.

The system clock can be scheduled to automatically switch to Daylight Savings Time (DST) based on a defined period of time in a specific year or a recurring period of time. Use the parameters in the **Daylight Savings** area to define a period of time in a specific year and use the parameters in the **Recurring** area to define a recurring period of time.

Daylight Savings — Click this check box to enable DST on the device based on the device geographical location. The possible field values are:

USA — The device clock changes to DST at 2 a.m. on the first Sunday of April, and reverts to standard time at 2 a.m. on the last Sunday of October.

European — The device clock changes to DST at 1:00 am on the last Sunday in March and reverts to standard time at 1:00 am on the last Sunday in October. This option applies to EU members and other European countries using the EU standard.

Other — The device clock changes to DST according to a user-defined range of time.

Time Set Offset (1-1440) — For countries outside the USA and Europe, the difference between Standard Time and DST can be set in minutes. The default time is 60 minutes.

From/To — Defines the date and time that DST begins/ends in countries outside the USA and Europe. The date format is DD/MMM/YY and the time format is HH:MM.

Recurring — Click this check box to enable DST on the device based on a recurring time frame. The possible field values are:

From/To — Defines the Day/Week/Month and time that DST begins/ends. The time format is HH:MM.

Selecting a Clock Source

1. Open the **Time Synchronization** page.
2. Define the **Clock Source** field.
3. Click **Apply Changes**.

   The Clock source is selected, and the device is updated.

Defining Local Clock Settings

1. Open the **Time Synchronization** page.
2. Define the fields in the **Local Settings** area.
3. Click **Apply Changes**.

   The local clock settings are applied, and the device is updated.

Defining Daylight Savings Time

1. Open the **Time Synchronization** page.
2. Define the fields in the **Daylight Saving** or **Reccuring** area.
3. Click **Apply Changes**.

   The Daylight Saving Time settings are applied, and the device is updated.

Defining Clock Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **Time Synchronization** page.

Table 6-2. Time Synchronization CLI Commands

CLI Command	Description
`clock source {sntp}`	Synchronizes the system time with an SNTP server clock.
`no clock source`	Synchronizes the system time with the device clock.
`clock timezone` *hours-offset* `[minutes` *minutes-offset*`] [zone` *acronym*`]`	Sets the time zone for display purposes.
`no clock timezone`	Sets the time to Coordinated Universal Time (UTC).
`clock summer-time recurring {usa | eu | {`*week day month hh:mm week day month hh:mm*`}} [offset` *offset*`] [zone` *acronym*`]`	Configures the system to automatically switch to Daylight Savings Time (DST) according to USA or European standards or according to a user-defined recurring time frame.
`clock summer-time date` *date month year hh:mm date month year hh:mm* `[offset` *offset*`] [zone` *acronym*`]`	Configures the system to automatically switch to DST during a user-defined period of time.
`no clock summer-time`	Configures the system not to switch to DST.
`show clock`	Displays the system clock time and date.
`show clock [detail]`	Displays the system clocks' time, date, time zone and Daylight Savings Time (DST) configuration.

The following is an example of CLI commands:

```
Console(config)# clock timezone -6 zone CST

Console(config)# clock summer-time recurring first sun apr 2:00
last sun oct 2:00
```

Configuring System Health Information

The **System Health** page displays physical device information, including information about the switch's power and ventilation sources. To display the **System Health** page, click **System→General→ Health** in the tree view.

Figure 6-4. System Health

The **System Health** page contains the following fields:

Power Supply—The power supply status.

— The power supply is operating normally.

— The power supply is not operating normally.

Not Present—The power supply is currently not present.

Fan—Indicates the fan status. The PowerConnect 6024/6024F has two fans.

— The fan is operating normally.

— The fan is not operating normally.

Not Present—A fan is currently not present.

Temperature—The temperature at which the device is currently running.

Viewing System Health Information Using the CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed on the **System Health** page.

Table 6-3. System Health CLI Commands

CLI Command	Description
`show system`	Displays system information.

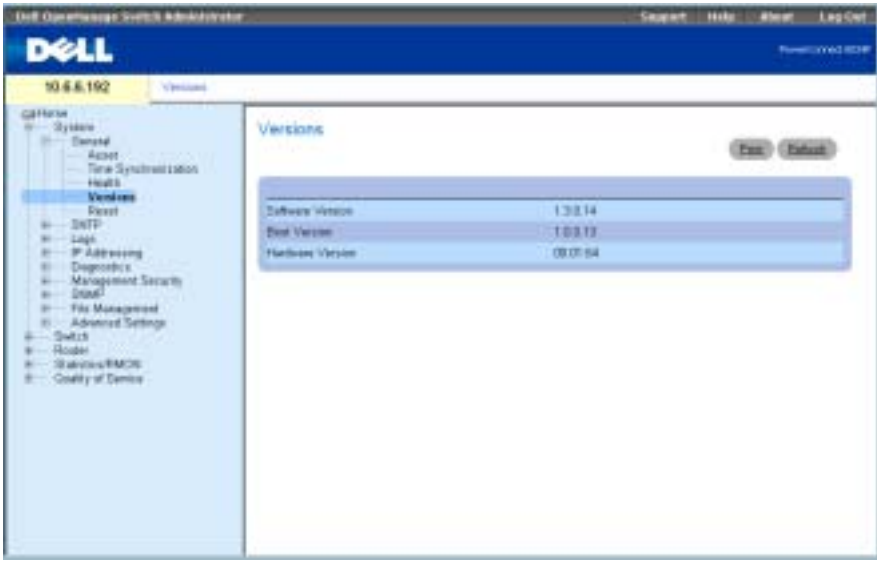
The following is an example of the CLI commands:

```
Console# show system

System Description:                    Ethernet Routing Switch
System Up Time (days,hour:min:sec):    0,00:32:04
System Contact:
System Name:
System Location:
System MAC Address:                    00:0d:56:2f:45:30
OOB MAC Address:                       00:00:00:00:00:18
System Object ID:                      1.3.6.1.4.1.674.10895.3000
Type:                                  PowerConnect 6024

Main Power Supply Status:              OK
Redundant Power Supply Status:         OK
Fan 1 Status:                          OK
Fan 2 Status:                          OK
Temperature (Celsius):                 45
Temperature Sensor Status:             OK
```

Version Information

The **Versions** page contains information about the hardware and software versions currently running. To display the **Versions** page, click **System→General→Versions** in the tree view (see Figure 6-5).

Figure 6-5. Versions



The **Versions** page contains the following fields:

Software Version—The current software version running on the device.

Boot Version—The current boot version running on the device.

Hardware Version—The current hardware version running on the device.

Displaying Device Versions Using the CLI

The following table summarizes the equivalent CLI command for viewing fields displayed in the **Versions** page.

Table 6-4. Versions CLI Command

CLI Command	Description
`show version`	Displays system version information.

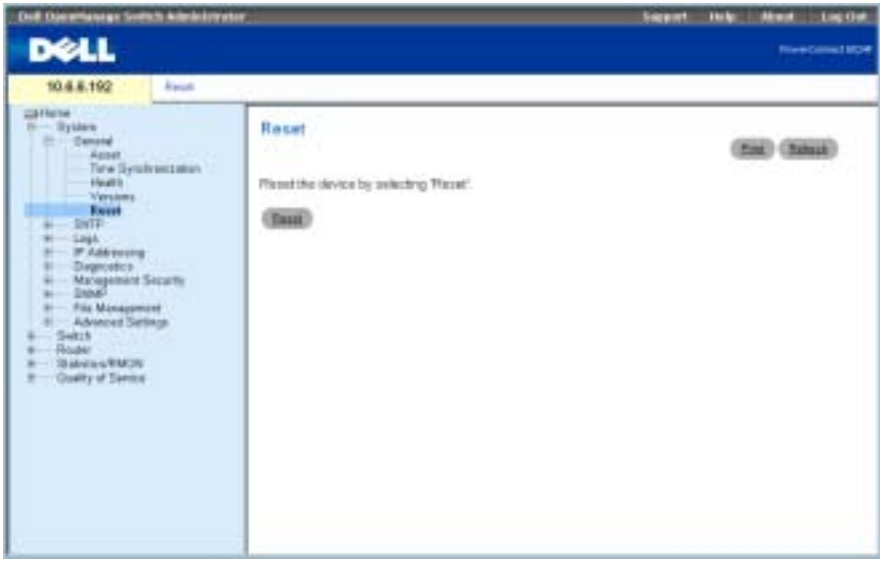
The following is an example of the CLI commands:

```
Console# show version

SW version    1.0.0.67 ( date  26-Jun-2003 time  18:15:42 )

Boot version    1.0.0.11 ( date  12-Jun-2003 time  15:55:01 )

HW version    00.01.64
```

Resetting the Device

You can use the **Reset** page to reset the device. To open the **Reset** page, click **System→General→ Reset** in the tree view (see Figure 6-6).

Figure 6-6. Reset



NOTE: Save all changes to the Running Configuration file before resetting the device to prevent the current device configuration from being lost. For information about saving Configuration files, see "Managing Files."

Resetting the Device

1. Open the **Reset** page.
2. Click **Reset**.
3. When the confirmation message displays, click **OK**.

   The device is reset. After the device is reset, enter a user name and password.

Resetting the Device Using the CLI

1. If you are not already in the Privileged User EXEC mode of the CLI, enter `enable`.
2. If you want to save any changes made to the running configuration of the device, enter `copy running-config startup-config`.
3. Enter `reload`.
4. Press `y` when asked if you want to continue.

Configuring SNTP Settings

The device supports the Simple Network Time Protocol (SNTP). SNTP assures accurate network device clock time synchronization up to the millisecond. Time synchronization is performed by a network SNTP server. The device operates only as an SNTP client and cannot provide time services to other systems.

Time sources are established by Stratums. Stratums define the accuracy of the reference clock. The higher the stratum (where zero is the highest), the more accurate the clock. The device receives time from stratum 1 and above.

The following is an example of stratums:

- **Stratum 0** — A real time clock is used as the time source, for example, a GPS system.
- **Stratum 1** — A server that is directly linked to a Stratum 0 time source is used. Stratum 1 time servers provide primary network time standards.
- **Stratum 2** — The time source is distanced from the Stratum 1 server over a network path. For example, a Stratum 2 server receives the time over a network link, via NTP, from a Stratum 1 server.

Information received from SNTP servers is evaluated based on the time level and server type.

SNTP time definitions are assessed and determined by the following time levels:

- **T1** — Time at which the original request was sent by the client.
- **T2** — Time at which the original request was received by the server.
- **T3** — Time at which the server sent a reply.
- **T4** — Time at which the client received the server's reply.

The device can poll the following server types for the server time: Unicast, Anycast and Broadcast.

Polling for Unicast information is used for polling a server for which the IP address is known. SNTP servers that have been configured on the device are the only ones that are polled for synchronization information. T1-T4 are used to determine server time. This is the preferred method for synchronizing device time because it is the most secure method. If this method is selected, SNTP information is accepted only from SNTP servers defined on the device using the **SNTP Servers** page.

Polling for Anycast information is used when the server IP address is unknown. If this method is selected, all SNTP servers on the network can send synchronization information . The device is synchronized when it proactively requests synchronization information. The best response (lowest stratum) from the first 3 SNTP servers to respond to a request for synchronization information is used to set the time value. Time levels T3 and T4 are used to determine the server time.

Using Anycast polling to get time information for synchronizing device time is preferred to using Broadcast polling to get time information. However, this method is less secure than unicast polling, because SNTP packets are accepted from SNTP servers that are not configured on the device.

Broadcast information is used when the server IP address is unknown. When a Broadcast message is sent from an SNTP server, the SNTP client listens to the message. If Broadcast polling is enabled, any synchronization information is accepted, even if it has not been requested by the device. This is the least secure method.

The device retrieves synchronization information, either by actively requesting information or at every poll interval. If Unicast, Anycast and Broadcast polling are enabled, the information is retrieved in this order:

- Information from servers defined on the device is preferred. If Unicast polling is not enabled or if no servers are defined on the device, the device accepts time information from any SNTP server that responds.
- If more than one Unicast device responds, synchronization information is preferred from the device with the lowest stratum.
- If the servers have the same stratum, synchronization information is accepted from the SNTP server that responded first.

MD5 (Message Digest 5) Authentication safeguards device synchronization paths to SNTP servers. MD5 is an algorithm that produces a 128-bit hash. MD5 is a variation of MD4, and increases MD4 security. MD5 verifies the integrity of the communication, authenticates the origin of the communication.

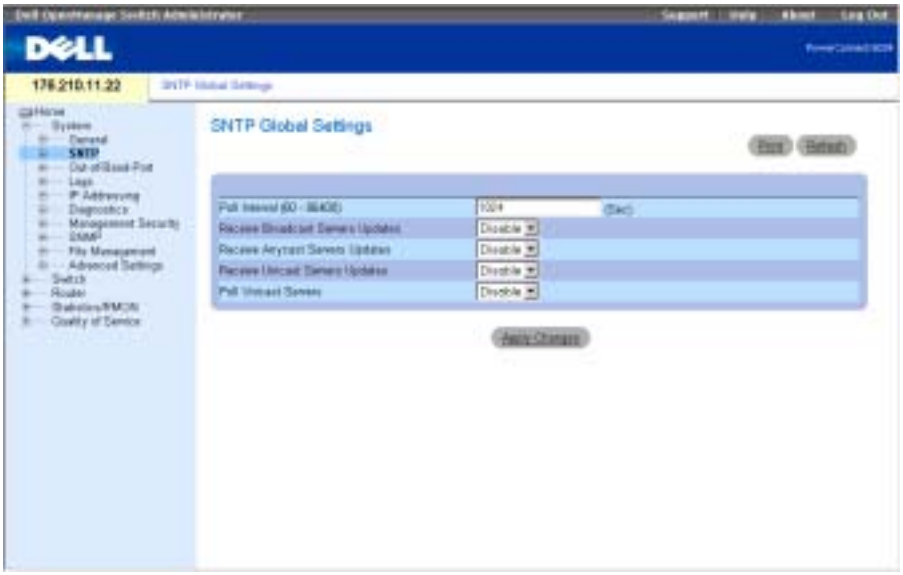
The **SNTP** page contains links to pages that allow network managers to configure SNTP parameters. To open the **SNTP** page, click **System→SNTP** in the tree view.

Defining SNTP Global Parameters

The **SNTP Global Settings** page provides information for defining SNTP parameters.

To open the **SNTP Global Settings** page, click **System →SNTP→Global Settings** in the tree view.

Figure 6-7. SNTP Global Settings



The **SNTP Global Settings** page contains the following fields:

Poll Interval (60-86400) — Defines the interval (in seconds) at which the SNTP server is polled for Unicast information.

Receive Broadcast Servers Updates — If enabled, listens to the SNTP servers for Broadcast server time information on the selected interfaces. The device is synchronized whenever an SNTP packet is received, even if synchronization was not requested.

Receive Anycast Servers Updates — If enabled, polls the SNTP servers for Anycast server time information. The device is synchronized only when a synchronization request is sent from the device.

Receive Unicast Servers Updates — If enabled, polls the SNTP servers defined on the device for Unicast server time information. If the **Receive Broadcast Servers Updates**, **Receive Anycast Servers Updates** and **Receive Unicast Servers Updates** fields are enabled, the system time is set according to the Unicast server time information.

Poll Unicast Servers — If enabled, sends SNTP Unicast server time information requests to the SNTP server.

Defining SNTP Global Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Global Settings** page.

Table 6-5. SNTP Global Parameters CLI Commands

CLI Command	Description
`sntp client poll timer` *seconds*	Sets the polling time for the SNTP client
`sntp broadcast client enable`	Enables SNTP Broadcast clients
`sntp anycast client enable`	Enables SNTP Anycast clients
`sntp unicast client enable`	Enables SNTP predefined Unicast clients
`sntp unicast client poll`	Enables polling pre-defined Unicast SNTP servers
`show sntp configuration`	Displays the SNTP configuration.
`show sntp status`	Displays the SNTP status.

The following is an example of the CLI commands:

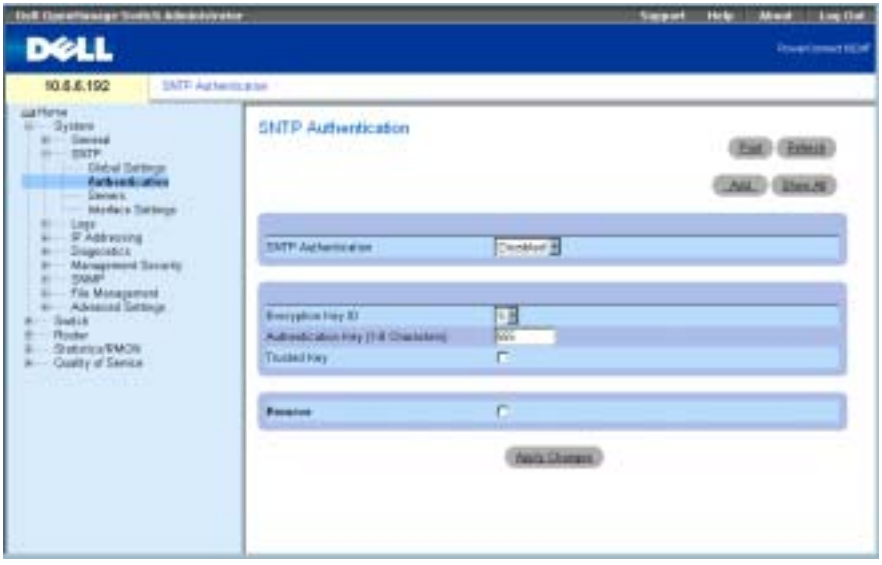
```
Console(config)# sntp anycast client enable
```

Defining SNTP Authentication Methods

The **SNTP Authentication** page enables SNTP authentication between the device and a SNTP server. The SNTP server is also selected in the **SNTP Authentication** page.

Click **System →SNTP→Authentication** in the tree view to open the **SNTP Authentication** page.

Figure 6-8. SNTP Authentication



The **SNTP Authentication** page contains the following fields:

SNTP Authentication — If enabled, requires authenticating an SNTP session between the device and an SNTP server.

Encryption Key ID — Contains a list of user-defined key IDs used to authenticate the SNTP server and device. Possible field values are 1 to 4294967295.

Authentication Key (1-8 Characters) — The key used for authentication.

Trusted Key — Check the check box to specify the encryption key used (Unicast/Anycast) or elected (Broadcast) to authenticate the SNTP server..

Remove — Check the check box to remove the selected authentication key.

Adding an SNTP Authentication Key

1. Open the **SNTP Authentication** page.
2. Click **Add**.

   The **Add Authentication Key** page opens:

Figure 6-9. Add Authentication Key

3 Define the fields.

4 Click **Apply Changes**.

The SNTP Authentication Key is added, and the device is updated.

Displaying the Authentication Key Table

1 Open the **SNTP Authentication** page.

2 Click **Show All**.

The **Authentication Key Table** page opens:

Figure 6-10. Authentication Key Table

Deleting an Authentication Key

1 Open the **SNTP Authentication** page.

2 Click **Show All**.

The **Authentication Key Table** page opens.

3 Select an **Authentication Key Table** entry.

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The entry is removed, and the device is updated.

Defining SNTP Authentication Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Authentication** page.

Table 6-6. SNTP Authentication CLI Commands

CLI Command	Description
`sntp authenticate`	Set to require authentication for received Network Time Protocol (NTP) traffic from servers.
`sntp authentication-key` *`number`* `md5` *`value`*	Defines an authentication key for SNTP.
`sntp trusted-key` *`key-number`*	Defines the authentication key used to authenticate the SNTP server.
`show sntp configuration`	Displays the SNTP configuration.

The following is an example of the CLI commands:

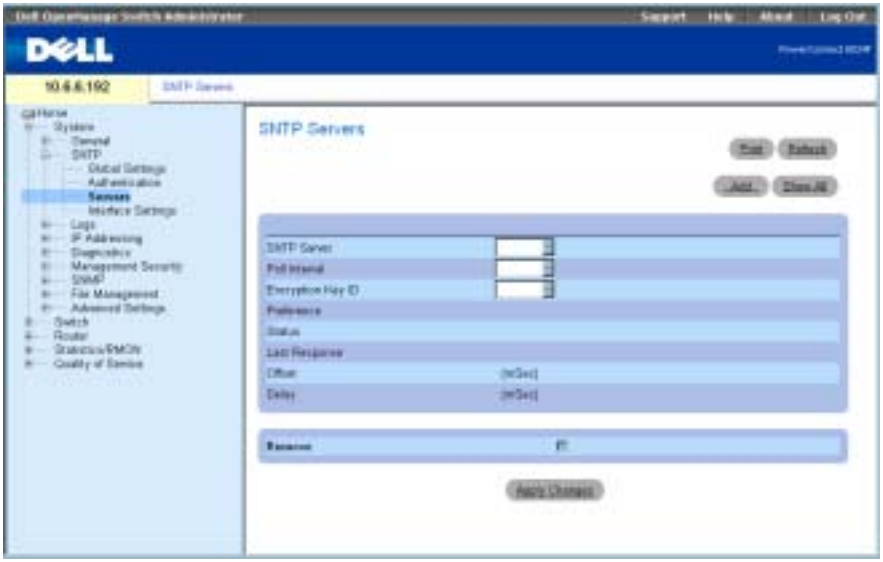
```
Console(config)# sntp authentication-key 8 md5 ClkKey
Console(config)# sntp trusted-key 8
Console(config)# sntp authenticate
```

Defining SNTP Servers

The **SNTP Servers** page contains information for enabling SNTP servers, as well as adding new SNTP servers.

To open the **SNTP Servers** page, click **System** →**SNTP** →**Servers** in the tree view.

Figure 6-11. SNTP Servers



The **SNTP Servers** page contains the following fields:

SNTP Server — Contains a list of user-defined SNTP server IP addresses. Up to eight SNTP servers can be defined.

Poll Interval — Enables polling the selected SNTP server for system time information, when enabled.

Encryption Key ID — Contains a list of user-defined key IDs used to communicate between the SNTP server and device. The Encryption Key ID is defined in the **SNTP Authentication** page.

Preference — The SNTP server providing SNTP system time information. The possible field values are:

Primary — The primary server provides SNTP information.

Secondary — The backup server provides SNTP information.

Status — The operating SNTP server status. The possible field values are:

Up — The SNTP server is currently operating normally.

Down — Indicates that a SNTP server is currently not available. For example, the SNTP server is currently not connected or is currently down.

In progress — The SNTP server is currently sending or receiving SNTP information.

Unknown — The progress of the SNTP information currently being sent is unknown. For example, the device is currently looking for an interface.

Last Response — The last time a response was received from the SNTP server.

Offset — Timestamp difference between the device's local clock and the acquired time from the SNTP server.

Delay — The amount of time it takes to reach the SNTP server.

Remove — Select the check box to remove a specific SNTP server from the **SNTP Servers** list.

Adding an SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Add.**

   The **Add SNTP Server** page opens:

Figure 6-12. Add SNTP Server

3. Define the fields.
4. Click **Apply Changes**.

   The SNTP server is added, and the device is updated.

Displaying the SNTP Servers Table

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** page opens:

Figure 6-13. SNTP Servers Table

Modifying an SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** opens.
3. Select an **SNTP Server** entry.
4. Modify the relevant fields.
5. Click **Apply Changes**.

   The SNTP server information is updated.

Deleting the SNTP Server

1. Open the **SNTP Servers** page.
2. Click **Show All.**

   The **SNTP Servers Table** opens.
3. Select an **SNTP Server** entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The entry is removed, and the device is updated.

Defining SNTP Servers Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Servers** page.

Table 6-7. SNTP Authentication CLI Commands

CLI Command	Description
`sntp server {`*`ip-address	hostname`*`} [poll] [key `*`keyid`*`]`	Defines an SNTP server that can be used for synchronizing time information.
`no sntp server `*`ip-address`*	Removes a server from the list of SNTP servers.

The following is an example of the CLI commands:

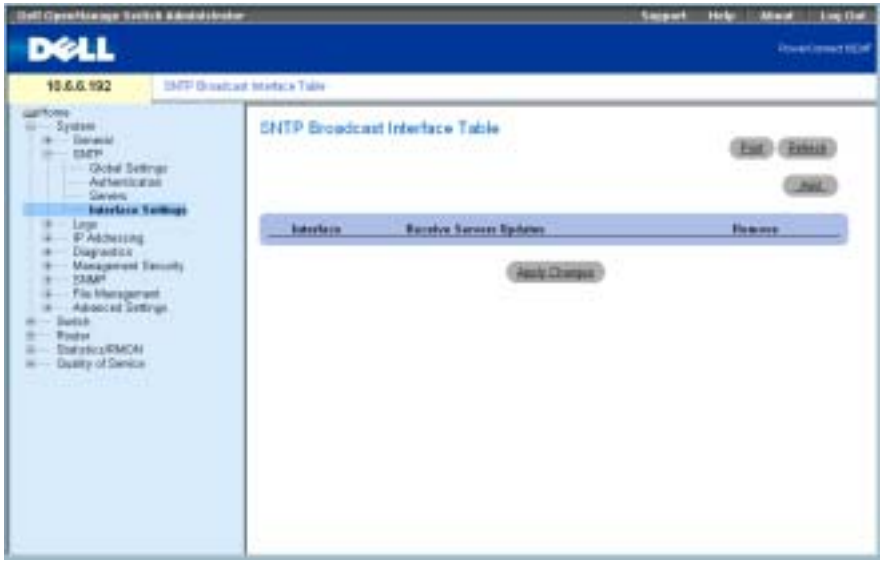
```
Console(config)# sntp server 100.1.1.1 poll key 10
```

Defining SNTP Interfaces

The **SNTP Broadcast Interface Table** contains fields for setting SNTP on different interfaces.

To open the **SNTP Broadcast Interface Table**, click **System→SNTP→Interfaces Settings**.

Figure 6-14. SNTP Broadcast Interface Table



The **SNTP Broadcast Interface Table** contains the following fields:

Interface — Displays a list of interfaces on which SNTP can be enabled.

Receive Servers Updates — Enables or disables receiving SNTP updates on the specific interface.

Remove — Select the check box to disable SNTP on the specific interface.

Enabling SNTP on an Interface

1. Open the **SNTP Broadcast Interface Table**.
2. Click **Add.**

   The **Add SNTP Interface** page opens.
3. Define the relevant fields.
4. Click **Apply Changes**.

   SNTP is enabled on the interface, and the device is updated.

Defining SNTP Interface Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for setting fields displayed in the **SNTP Broadcast Interface Table**.

NOTE: When defining Anycast or Broadcast interfaces, at least one IP address must be defined.

Table 6-8. SNTP interface Settings CLI Commands

CLI Command	Description
`sntp client enable`	Enables the Simple Network Time Protocol (SNTP) broadcast and anycast client on an interface.
`show sntp configuration`	Displays the SNTP configuration.

The following is an example of the CLI commands for configuring SNTP interfaces:

```
Console (config)# interface ethernet g1
Console (config-if)# sntp client enable
Console (config-if)# end
Console# show sntp configuration
Polling interval: 7200 seconds.

MD5 Authentication keys: 8, 9
Authentication is required for synchronization.
Trusted Keys: 8,9

Unicast Clients Polling: Enabled.

Server           Polling          Encryption Key
-----------      --------         -----------------
176.1.1.8        Enabled          9
176.1.8.179      Disabled         Disabled

Broadcast Clients: Enabled
Broadcast Clients Poll: Enabled
Broadcast Interfaces: g1
```

Configuring Out-of-Band (OOB) Management Ports

This section describes managing the following device features through the Out-of-Band management port. It includes information about the the Out-of-Band remote log server, Out-of-Band default gateway, Out-of-Band IP interface parameters, Out-of-Band TACACS+ server and Out-of-Band RADIUS server.

When managing these features using the Out-of-Band management port, in-band management of these features is disabled. Use the SNMP interface to configure these features via the Out-of-Band port.

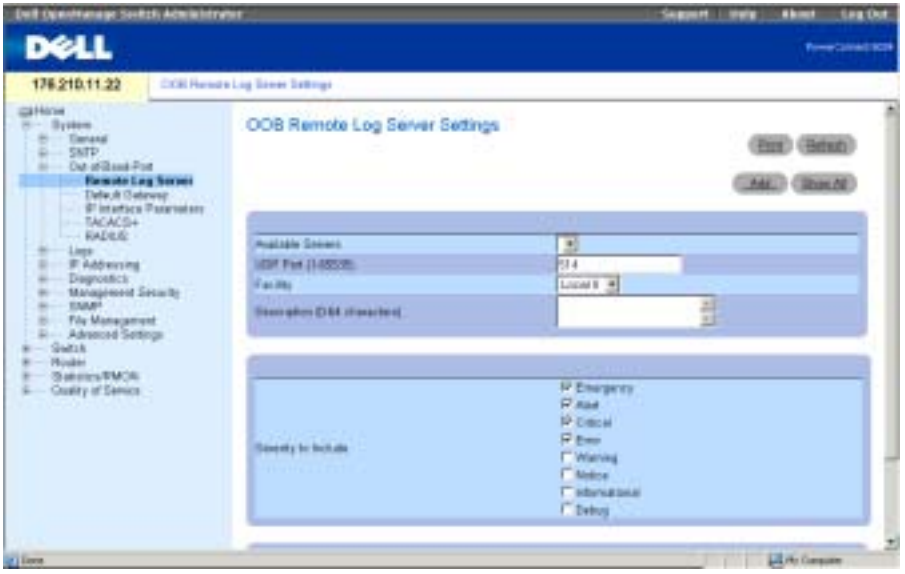
To open the **OOB Configuration** page, click **System→Out of Band** in the tree view.

Configuring Out-of-Band Remote Log Servers

The **OOB Remote Log Server Settings** page contains fields for viewing the available out-of-band port log servers. In addition, new Out-of-Band log servers can be defined, and the severity of the logs sent to the sever.

To open the **OOB Remote Log Server Settings** page, click **System→Out-of-Band Port→Remote Log Server** in the tree view.

Figure 6-15. OOB Remote Log Server Settings



The **OOB Remote Log Server Settings** page contains the following fields:

Available Servers—Servers to which logs can be sent.

UDP Port (1-65535)—The UDP port from which the logs are sent. The default value is 514.

Facility—A user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device use the same facility on a server. The possible field values are local 0, local 1, local 2, local 3, local 4, local 5, local 6 and local 7.

Description (0-64 characters)—Displays the user-defined server description.

Severity to Include—The log severity. Selecting a severity level automatically selects all higher severity levels.

Delete Server—When checked, deletes a server from the **Available Servers** list.

The **OOB Remote Log Server Settings** page also contains a severity list. The severity definitions are the same as the severity definitions on the RAM Log Table on page 138.

Sending Logs to an Out-of-Band Log Server

1. Open the **OOB Remote Log Server Settings** page.
2. Define the **UDP Port**, **Facility**, and **Description** fields.
3. Select the log type and log severity.
4. Click **Apply Changes**.

   The log settings are saved, and the device is updated.

NOTE: Before adding a new server, determine the IP address of the Out-of-Band remote log server.

Defining a New Out-of-Band Log Server

1. Open the **OOB Remote Log Server Settings** page.
2. Click **Add** to display the **Add an OOB Log Server** page.
3. Complete the fields in the dialog.
4. Click **Apply Changes**.

   The server is defined and added to the **Available Servers** List.

Deleting an Out-of-Band Log Server

1. Open the **OOB Remote Log Server Settings** page.
2. Click **Show All** to display the **OOB Remote Log Servers Table** page.
3. Select a server and check the **Remove** checkbox.
4. Click **Apply Changes**.

   The server is deleted, and the device is updated.

Configuring Out-of-Band Remote Server Logs Using the CLI Commands

The following table summarizes the CLI commands for working with fields in the **OOB Remote Log Server Settings** page.

Table 6-9. Out-of-Band Remote Log Server Settings CLI Commands

CLI Command	Description
`logging` *oob/ip-address* `[port` *port*`]` `[severity` *level*`]` `[facility` *facility*`]` `[description` *text*`]`	Defines a new remote log server.

The following is an example of the CLI commands:

```
Console(config)#logging oob/10.2.2.2  severity critical facility
local0 description syslog_server_1
```

Defining Out-of-Band Default Gateways

Use the **OOB Default Gateway** page to assign gateway devices. Packets are forwarded to the default IP when frames are sent to a remote network. The configured IP address must belong to the same IP address subnet of one of the IP interfaces. Removing the IP interface to which a default gateway is connected, also removes the default gateway.

To open the **OOB Default Gateway** page, click **System →Out-of-Band Port→Default Gateway** in the tree view.

Figure 6-16. OOB Default Gateway

The **OOB Default Gateway** page contains the following parameter:

Default Gateway—Indicates the gateway device IP address.

Selecting a Out-of-Band Gateway Device

1 Open the **OOB Default Gateway** page.

2 Define an IP address in the **Default Gateway** field.

3 Click **Apply Changes**.

The Out-of-Band Gateway device is defined, and the device is updated.

Table 6-10. Out-of-Band Default Gateway CLI Commands

CLI Command	Description
`ip default gateway` *ip-address*	Defines the Out-of-Band IP Gateway.

The following is an example of the CLI commands:

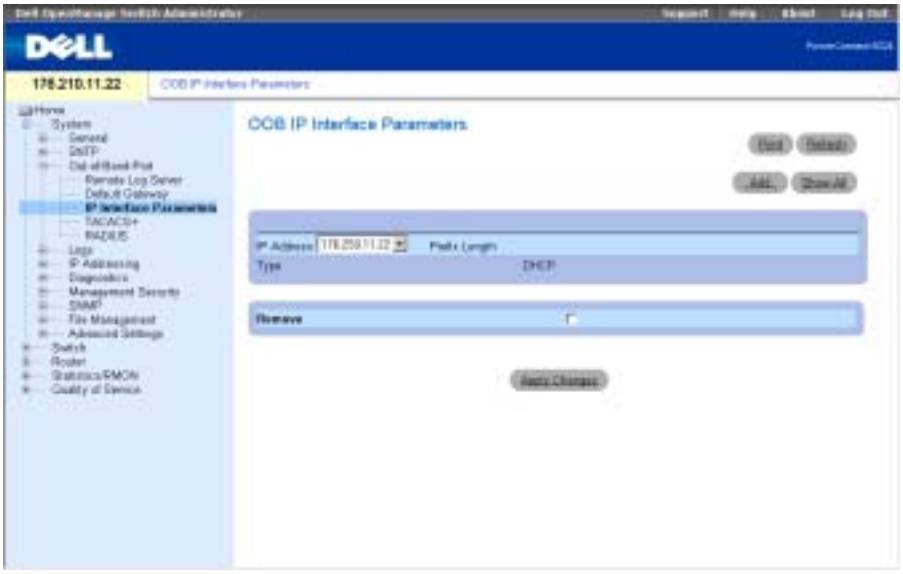
```
Console(config)# interface out-of-band-eth
Console(config-oob)# ip address 10.0.0.1 /8
Console(config-oob)# ip default-gateway 10.1.1.1
```

Defining Out-of-Band IP Interface Parameters

The **OOB IP Interface Parameters** page contains parameters for assigning Out-of-Band IP addresses to interfaces.

To open the **OOB IP Interface Parameters** page, click **System→Out-of-Band Port→IP Interface Parameters** in the tree view.

Figure 6-17. OOB IP Interface Parameters



The **OOB IP Interface Parameters** page contains the following parameters:

IP Address—The Out-of-Band interface IP address.

Prefix Length—The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

Type—The means by which the Out-of-Band IP interface was created; DHCP or static.

Remove—When checked, removes the interface from the **IP Address** drop-down list.

NOTE: You can configure DHCP IP addresses for Out-of-Band management on the **DHCP IP Interface** page (**System→IP Address→DHCP IP Interface**).

Adding an IP Interface

1. Open the **OOB IP Interface Parameters** page.
2. Click **Add** to display the **Add a Static OOB IP Interface** page.
3. The **Network Mask** field specifies the subnetwork mask of the source IP address.
4. Complete the fields in the page.
5. Click **Apply Changes**.

   The new interface is added, and the device is updated.

Deleting IP Addresses

1. Open the **OOB IP Interface Parameters** page.
2. Click **Show All**.
3. The **Interface Parameters Table** page opens.
4. Select an IP address in the **IP Address** drop-down list.
5. Select an entry in the **Interface Parameters Table**.
6. Check the **Remove** checkbox.
7. Click **Apply Changes**.

   The IP address is deleted, and the device is updated.

Defining IP Interfaces Using CLI Commands

The following table summarizes the CLI commands for working with fields in the **OOB IP Interface Parameters** page.

Table 6-11. Out-of-Band IP Interface Parameters CLI Commands

CLI Command	Description
`interface out-of-band-eth`	Configures the out-of-band Ethernet port and sets the interface configuration mode.
`ip address` *`ip-address`* {*`mask`* | *`prefix-length`*}	Sets an IP address.

The following is an example of the CLI commands:

```
Console# configure
Console(config)# interface out-of-band-eth
Console(config-oob)# ip address 192.168.0.1 /8
```

Configuring Out-of-Band TACACS+ Servers

The device provides Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

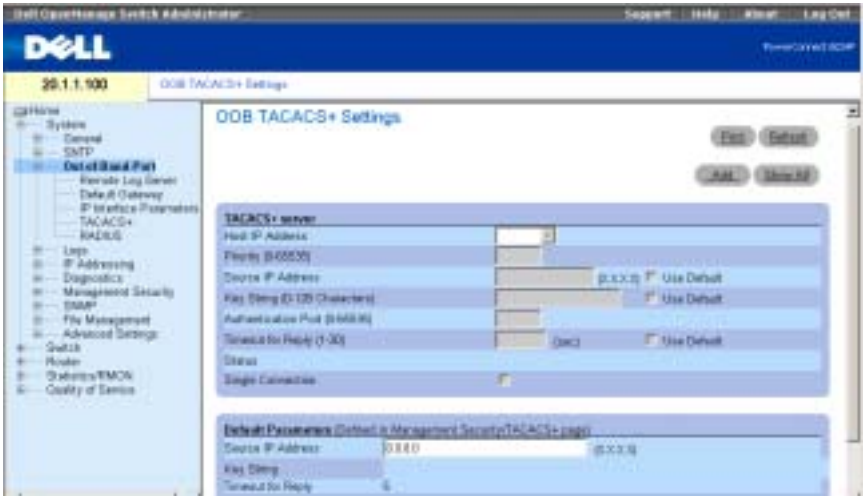
TACACS+ servers can be defined on in-band ports using **TACACS+ Settings** page or on the out-of-band port.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

The **OOB TACACS+ Settings** page contains both user-defined and the default TACACS+ settings for the Out-of-Band management port.

To open the **OOB TACACS+ Settings** page, click **System→Out-of-Band-Port→TACACS+** in the tree view.

Figure 6-18. OOB TACACS+ Settings



The **OOB TACACS+ Settings** page contains the following fields:

Host IP Address — Specifies the TACACS+ Server IP address.

Priority (0-65535) — Specifies the order in which the TACACS+ servers are used. The default is 0.

Source IP Address — The device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server.

Authentication Port (0-65535) — The port number through which the TACACS+ session occurs. The default is port 49.

Reply Timeout (1-30) — The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.

Status — The connection status between the device and the TACACS+ server. The possible field values are:

Connected — There is currently a connection between the device and the TACACS+ server.

Not Connected — There is not currently a connection between the device and the TACACS+ server.

Single Connection — Maintains a single open connection between the device and the TACACS+ server when selected

The TACACS+ default parameters are user-defined defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ servers. The following are the TACACS+ defaults:

Source IP Address — The default device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — The default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.

Timeout for Reply (1-30) — The default time that passes before the connection between the device and the TACACS+ times out.

NOTE: You can set the values for the aforementioned defaults on the **TACACS+ Settings** page (**System→Management Security→TACACS+**).

Defining TACACS+ Parameters

1. Open the **OOB TACACS+ Settings** page.
2. Define the fields.
3. Click **Apply Changes**.

   The TACACS+ settings are updated to the device.

Adding a TACACS+ Server

1. Open the **OOB TACACS+ Settings** page.
2. Click **Add**.

   The **Add OOB TACACS+ Host** page opens.
3. Define the fields.
4. Click **Apply Changes**.

   The TACACS+ server is added, and the device is updated.

Deleting a TACACS+ Server from the TACACS+ Servers List

1. Open the **OOB TACACS+ Settings** page.
2. Click **Show All**.

The **TACACS+ Table** page opens.

3 Select a **TACACS+ Table** entry.

4 Select the **Remove** check box.

5 Click **Apply Changes**.

The TACACS+ server is removed, and the device is updated.

Defining TACACS+ Servers Using CLI Commands

The following table summarizes the CLI commands for working with fields in the **OOB TACACS+ Settings** page.

Table 6-12. Out-of-Band TACACS+ Settings CLI Commands

CLI Command	Description
tacacs-server host {*oob/ip-address* / *hostname*} [single-connection] [port *port-number*] [timeout *timeout*] [key *key-string*] [source *source*] [priority *priority*]	**Specifies a TACACS+ server host.**
no tacacs-server host {*ip-address* / *hostname*}	**Deletes a specified TACACS+ server host.**
`tacacs-server key [key-string]`	**Specifies the authentication and encryption key used for all TACAS communication between the device and the TACACS+ server. This key must match the encryption used on the TACACS daemon. (Range:0-128 characters)**
`no tacacs-server key`	**Returns to the default.**
`tacacs-server timeout timeout`	**Specifies the timeout value in seconds. (Range: 1-30)**
`no tacacs-server timeout`	**Returns to the default.**
`tacacs-server source-ip` ***oob/ip-address***	**Specifies the source IP address. (Range: Valid IP address)**
no `tacacs-server source-ip` ***oob/ip-address***	**Returns to the default.**
show tacacs [oob/ip-address]	**Displays configuration and statistics for a TACACS+ server.**

The following is an example of the CLI commands:

```
Console(config)# tacacs-server host oob/172.16.8.1 key abc
Console (config)# end
Console# show tacacs

Device Configuration
--------------------
IP address  Status     Port  Single      TimeOut   Source  Priority
                           Connection            IP
----------  ---------  ----  ----------  --------  ------  --------
No TACACS server is configured.

OOB host Configuration
IP address  Status     Port  Single      TimeOut   Source  Priority
                           Connection            IP
----------  ---------  ----  ----------  --------  ------  --------
172.16.8.1  Not        49    No          Global    Global  0
            Connected

Global Values
-------------
TimeOut: 5

Device Configuration
--------------------
Source IP: 0.0.0.0

OOB host Configuration
----------------------
Source IP : 0.0.0.0
```

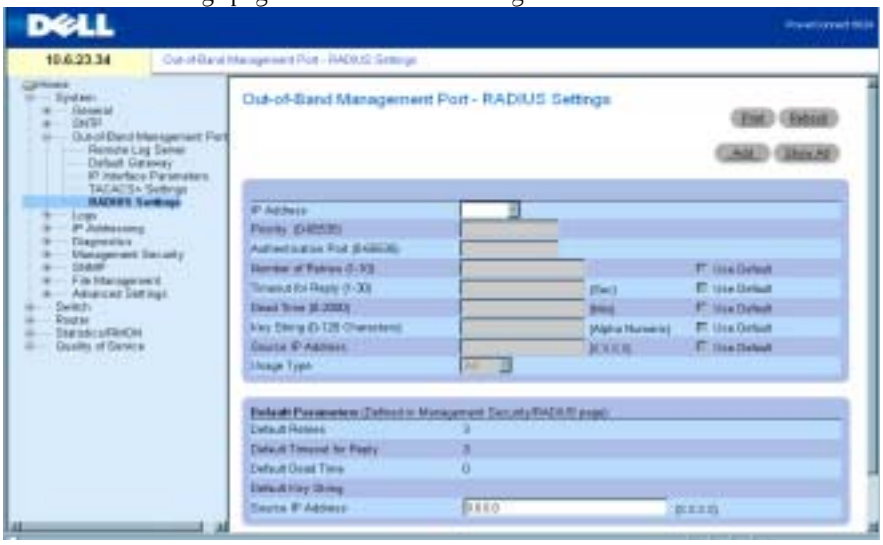
Configuring Out-of-Band RADIUS Servers

The **OOB RADIUS Settings** page contains both user-defined and the default RADIUS settings for the Out-of-Band management port. For more information on RADIUS servers, see "Configuring TACACS+ Settings."

To open the **OOB RADIUS Settings** page, click **System→Out-of-Band Port→RADIUS** in the tree view (see OOB RADIUS Settings, Figure 6-19).

Figure 6-19. OOB RADIUS Settings

The **OOB RADIUS Settings** page contains the following fields:



IP Address—The Authentication Out-of-Band port IP address.

Priority (0-65535)—The Out-of-Band port priority. The possible values are 0-65535.

Authentication Port—The authentication port, which is used to verify the RADIUS server authentication.

Number of Retries (1-10)—Number of transmitted requests sent to the RADIUS server before a failure occurs. The possible field values are 1-10. The default value is 3. If no host-specific value is specified, the global value applies to each host.

Timeout for Reply (1-30)—Amount of time in seconds the device waits for an answer from the RADIUS server before timing out. The possible field values are 1-30. The default value is 3. If no host-specific value is specified, the global value applies to each host.

Dead Time (0-2000)—Amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. If no host-specific value is specified, the global value applies to each host.

Key String (0-128 Characters)—Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption. If no host-specific value is specified, the global value applies to each host.

Source IP Address—IP address of device accessing the RADIUS server.

The RADIUS default parameters are user-defined defaults. The default settings are applied to newly defined RADIUS servers. If default values are not defined, the system defaults are applied to the new RADIUS servers. The following are the RADIUS defaults:

Default Timeout for Reply—Default amount of the time the device waits for an answer from the RADIUS server before timing out.

Default Retries (sec)—Default number of transmitted requests sent to RADIUS server before a failure occurs.

Default Dead Time (sec)—Default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Default Key String—Default key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption.

NOTE: You can set the values for the aforementioned defaults on the **RADIUS Settings** page (**System→ Management Security→RADIUS**).

Source IP Address—Default IP address of a device accessing the RADIUS server.

Defining Out-of-Band RADIUS Parameters

1. Open the **OOB RADIUS Settings** page.
2. Define the the following fields: **Default Timeout for Reply**, **Default Retries**, **Default Dead Time**, and **Default Key**.
3. Click **Apply Changes**.

   The RADIUS settings are updated to the device.

Adding an Out-of-Band RADIUS Server

1. Open the **OOB RADIUS Settings** page.
2. Click **Add** to display the **Add OOB RADIUS Server** page.
3. Complete the fields in the dialog.
4. Click **Apply Changes**.

   The new RADIUS server is added, and the device is updated.

Deleting an Out-of-Band RADIUS Server from the RADIUS Servers List

1. Open the **OOB RADIUS Settings** page.
2. Click **Show All** to display the **OOB RADIUS Servers** list.

3 Select a RADIUS server and check the **Remove** checkbox.

4 Click **Apply Changes**.

The RADIUS server is removed from the RADIUS Servers list.

Defining RADIUS Servers Using CLI Commands

The following table summarizes the CLI commands for working with fields in the **OOB RADIUS Settings** page.

Table 6-13. Out-of-Band RADIUS Settings CLI Commands

CLI Command	Description
`radius-server host` *ip-address* `[auth-port` *auth-port-number*`] [timeout` *timeout*`] [retransmit retries] [deadtime` *deadtime*`] [key` *key-string*`] [source` *source*`] [priority` *priority*`]`	Specifies a RADIUS server host.
`no radius-server host` *ip-address*	Deletes a specified RADIUS server host.
`radius-server source-ip` *source*	Specifies the source IP address that is used for communication with RADIUS servers.
`no radius-server-ip`	Returns to default.
`radius-server timeout` *timeout*	Sets the interval for which a router waits for a server host to reply.
`no radius-server deadtime`	Sets the dead time to 0.

The following is an example of the CLI commands:

```
console(config)#interface out-of-band eth 1
console radius-server host oob/10.2.2.2 key 123
```

Managing Logs

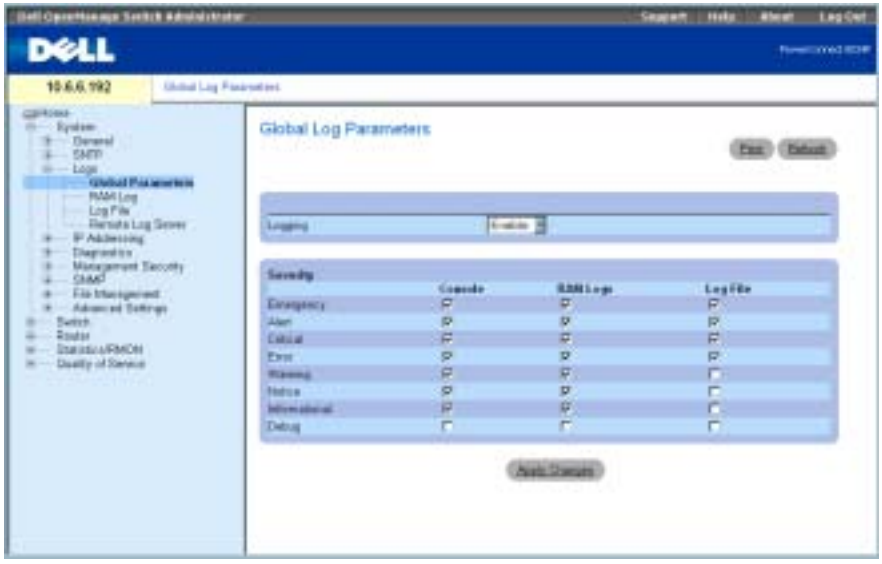
The **Logs** page contains links to various log pages. To display the **Logs** page, click **System→Logs** in the tree view.

Global Log Parameters

The **Global Log Parameters** page contains fields for enabling logs globally, and fields for defining log parameters. The **Severity** log messages are listed from the highest severity to the lowest.

To open the **Global Log Parameters** page, click **System→Logs→Global Parameters** in the tree view.

Figure 6-20. Global Log Parameters



The **Global Log Parameters** page contains the following fields:

Logging — Enables device global logs for Cache, File, and Server Logs. All logs which are printed to the console are saved to the log files. The possible field values are:

Enable — Enables saving logs in Cache (RAM), File (FLASH), and an External Server.

Disable — Disables saving logs. It is not possible to disable logging of logs that are printed to console.

Emergency — The highest level warning level. If the device is down or not functioning properly, an emergency log is saved to the device.

Alert — The second highest warning level. An alert log is saved if there is a serious device malfunction, such as all device features being down.

Critical — The third highest warning level. A critical log is saved if a critical device malfunction occurs, for example, two device ports are not functioning, while the rest of the device ports remain functional.

Error — A device error has occurred, such as if a port is offline.

Warning — The lowest level of a device warning.

Notice — Provides the network administrators with device information.

Informational—Provides device information.

Debug — Provides detailed information about the log. Debugging should only be entered by qualified support personnel.

The check boxes appear under the following three columns:

Console — Logs sent to the console.

RAM Logs — Logs sent to the (Cache) RAM.

Log File — Logs sent to the File (FLASH).

Enabling Logs

1. Open the **Global Log Parameters** page.
2. Select **Enable** in the **Logging** drop-down menu.
3. Use the check boxes to select log type and severity.

NOTE: When you select a severity level, all higher severity levels are automatically selected.

4. Click **Apply Changes**.

   The log settings are saved, and the device is updated.

Enabling Global Logs Using the CLI

The following table summarizes the equivalent CLI commands for working with fields displayed in the **Global Log Parameters** page.

Table 6-14. Global Log Parameters CLI Commands

CLI Command	Description
`logging on`	Enables error message logging.
`logging` *ip-address* `[port` *port*`]` `[severity` *level*`]` `[facility` *facility*`]` `[description` *text*`]`	Logs messages to a syslog server.
`logging console` *level*	Limits messages logged to the console based on severity.
`logging buffered` *level*	Limits syslog messages displayed from an internal buffer (RAM) based on severity.
`logging file [`*level*`]`	Limits syslog messages sent to the logging file based on severity.

The following is an example of the CLI commands:

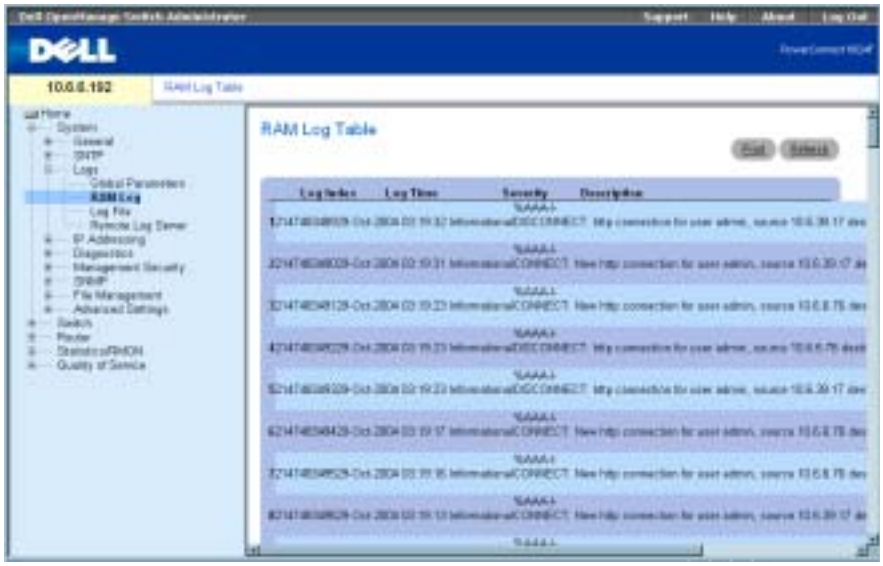
```
Console (config)# logging on
Console (config)# logging 10.1.1.1 severity critical
Console (config)# logging console errors
Console (config)# logging buffered debugging
Console (config)# logging file alerts

Console # clear logging
Clear Logging Buffer [y/n]? y
```

RAM Log Table

The **RAM Log Table** contains information about specific RAM (cache) log entries, including the time the log was entered, the log severity, and a description of the log.

To display the **RAM Log Table**, click **System→Logs→RAM Log** in the tree view (see Figure 6-21).

Figure 6-21. RAM Log Table



The **RAM Log Table** contains the following fields:

Log Index—Indicates the Log Number within the Log RAM Table.

Log Time—The time at which the log was entered in the Log RAM Table.

Severity—The log severity.

Description—The log description.

Removing Log Information

1. Open the **RAM Log Table** page.
2. Click **Clear Logs**.

   The log information is removed from the log file table, and the device is updated.

Viewing the RAM Log Table Using the CLI

The following table summarizes the equivalent CLI commands for viewing fields displayed in the RAM Log Table.

Table 6-15. RAM Log Table CLI Commands

CLI Command	Description
`show logging`	Displays the state of logging and the syslog messages stored in the internal buffer.
`clear logging`	Clears messages from the logging buffer.

The following is an example of the CLI commands:

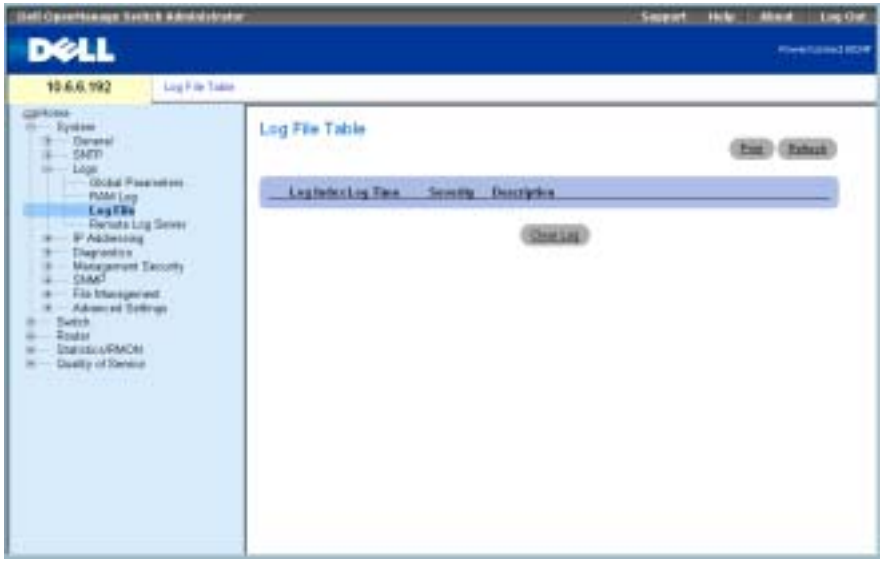
```
Console # show logging

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30
Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from
143.166.155.18


10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection
from 143.166.155.18 terminated


10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from
143.166.155.18

10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup
```

Log File Table

The **Log File Table** contains information about specific log entries, including the time the log was entered, the log severity, and a description of the log.

To display the **Log File Table**, click **System→Logs→Log File** in the tree view (see Table 6-22).

Figure 6-22. Log File Table



The **Log File Table** page contains the following fields:

- **Log Index**—The Log Number within the Log File Table.
- **Log Time**—The time at which the log was entered in the Log File Table.
- **Severity**—The log severity.
- **Description**—The log description.

Displaying the Log File Table Using the CLI

The following table summarizes the equivalent CLI commands for viewing fields displayed on the **Log File Table** page.

Table 6-16. Log File Table CLI Commands

CLI Command	Description
`show logging file`	Displays the state of logging and the syslog messages stored in the logging file.
`clear logging`	Clears messages from the logging buffer.

The following is an example of the CLI commands:

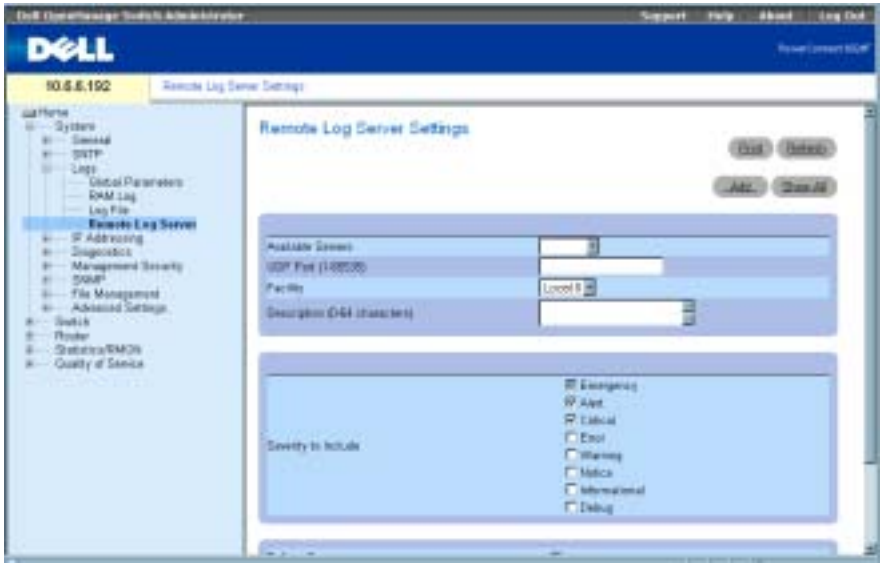
```
Console # show logging file

Console Logging: Level info. Console Messages: 0 Dropped.

Buffer Logging: Level info. Buffer Messages: 30 Logged, 30
Displayed, 200 Max.

File Logging: Level error. File Messages: 1 Logged, 30 Dropped.

1 messages were not logged

10-Jan-2003 16:53:44 :%MSCM-I-NEWTERM: New TELNET connection from
143.166.155.18


10-Jan-2003 16:53:14 :%MSCM-I-TERMTERMINATED: TELNET connection
from 143.166.155.18 terminated


10-Jan-2003 16:41:26 :%MSCM-I-NEWTERM: New TELNET connection from
143.166.155.18


10-Jan-2003 09:24:59 :%INIT-I-Startup: Cold Startup


10-Jan-2003 09:22:51 :%LINK-I-Up:  Oob-eth 1


10-Jan-2003 09:22:51 :%LINK-W-Down:  g24


10-Jan-2003 09:22:51 :%LINK-W-Down:  g23


10-Jan-2003 09:22:51 :%LINK-W-Down:  g22


10-Jan-2003 09:22:51 :%LINK-W-Down:  g21
```

Remote Log Server

The **Remote Log Server Settings** page contains fields for viewing the available log servers. In addition, new log servers can be defined, and the severity of the logs sent to the server.

To open the **Remote Log Server Settings** page, click **System→Logs→Remote Log Server**.

Figure 6-23. Remote Log Server Settings



The **Remote Log Server Settings** page contains the following fields:

Available Servers — Servers to which logs can be sent.

UDP Port (1-65535) — The UDP port from which the logs are sent. The default value is 514.

Facility — A user-defined application from which system logs are sent to the remote server. Only one facility can be assigned to a single server. If a second facility level is assigned, the first facility level is overridden. All applications defined for a device use the same facility on a server. The possible field values are **Local 0** - **Local 7**.

Description—The server description. The maximum length is 64 characters.

Severity — The log severity. Selecting a severity level automatically selects all higher severity levels.

Delete Server — Deletes a server from the **Available Server** list. Checking the check box deletes the server from the list. Leaving the box unchecked maintains the server in the list.

The **Remote Log Server Settings** page also contains a severity list. The severity definitions are the same as the severity definitions on the **RAM Log Table** page.

Sending Logs to a Server

1. Open the **Remote Log Server Settings** page.
2. Define the **UDP Port**, **Facility**, and **Description** fields.
3. Select the log type and log severity by using the **Log Parameters** check boxes.

NOTE: When you select a severity level, all higher severity levels are automatically selected.

4 Click **Apply Changes**.

The log settings are saved, and the device is updated.

Defining a New Server

1 Open the **Remote Log Server Settings** page.

2 Click **Add** to display the **Add a Log Server** page.

NOTE: Before adding a new server, determine the IP address of the remote log server.

3 Complete the fields in the dialog and click **Apply Changes**.

The **Remote Log Server Settings** page displays the server in the **Available Server** list only after you manually refresh the page.

Deleting a Log Server

1 Open the **Remote Log Server Settings** page.

2 Click **Show All** to open the **Log Server Table** page.

3 Select a server and check the **Remove** check box.

4 Click **Apply Changes**.

The server is deleted, and the device is updated.

Working with Remote Server Logs Using the CLI Commands

The following table lists the CLI commands for working with remote server logs.

Table 6-17. Remote Log Server CLI Commands

CLI Command	Description
`logging` *`ip-address`* `[port port] [severity` *`level`*`] [facility` *`facility`*`] [`*`description text`*`]`	Logs messages to a remote server.

The following is an example of the CLI commands:

```
Console (config) # logging 10.1.1.1 severity critical
```

Defining IP Addressing

Use the **IP Addressing** page to assign interface and default gateway IP addresses, and define ARP and DHCP parameters for the interfaces.

To open the **IP Addressing** page, click **System→IP Addressing** in the tree view.

Defining IP Interfaces

The **IP Interface Parameters** page contains parameters for assigning IP addresses to interfaces.

To open the **IP Interface Parameters** page, click **System→IP Addressing→Interface Parameters** in the tree view.

Figure 6-24. IP Interface Parameters

The **IP Interface Parameters** page contains the following fields:

IP Address — The interface IP address.

Prefix Length — The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

Interface — The interface type for which the IP address is defined. The possible field values are **Port**, **LAG**, or **VLAN**.

For information about configuring Link Aggregated Groups (LAGs), see "Aggregating Ports." For information about configuring VLANs, see "Configuring VLANs."

Type — Indicates whether or not the IP address was configured statically.

Forward Directed IP Broadcasts — Enables the translation of a directed broadcast to physical broadcasts. Disabling drops IP-directed broadcasts and does not forward them.

Broadcast Type — Defines an interface broadcast address.

One Fill indicates the interface broadcast address is one fill (255.255.255.255).

Zero Fill indicates the interface broadcast address is zero fill (0.0.0.0).

Remove — When checked, removes the interface from the **IP Address** drop-down menu.

Adding an IP Interface

1. Open the **IP Interface Parameters** page.
2. Click **Add** to open the **Add a Static IP Interface** page.

Figure 6-25. Add a Static IP Interface

3. Complete the fields on the page.

   Network Mask specifies the subnetwork mask of the source IP address.

Each part of the IP address must start with a number other than zero. For example, IP addresses 001.100.192.6 and 192.001.10.3 are invalid.

4. Click **Apply Changes**.

   The new interface is added, and the device is updated.

Modifying IP Address Parameters

1. Open the **IP Interface Parameters** page.
2. Select an IP address in the **IP Address** drop-down menu.
3. Modify the required fields.
4. Click **Apply Changes**.

   The parameters are modified, and the device is updated.

Deleting IP Addresses

1. Open the **IP Interface Parameters** page.
2. Click **Show All** to display the **Interface Parameters Table** page.
3. Select an IP address and check the **Remove** check box.
4. Click **Apply Changes**.

   The IP address is deleted, and the device is updated.

Defining IP Interface Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for working with fields on the **IP Interface Parameters** page.

Table 6-18. IP Interface Parameters CLI Commands

CLI Command	Description
`ip address` *ip-address* `{mask | prefix-length}`	Sets an IP address.
`no ip address [`*ip-address*`]`	Removes an IP address
`show ip interface [ethernet` *s* `| vlan` *vlan-id* `|` *port-channel number*`]`	Displays the usability status of interfaces configured for IP.
`directed-broadcast`	Enables the translation of a directed broadcast to physical broadcasts.

The following is an example of the CLI commands:

```
Console (config)# interface vlan 1
Console (config-if)# ip address 192.168.1.1 255.255.255.0
Console (config-if)# no ip address 192.168.1.1
```

Defining DHCP IP Interface Parameters

The **DHCP IP Interface** page specifies the DHCP clients connected to the device.

To open the **DHCP IP Interface** page, click **System→IP Addressing→DHCP IP Interface** in the tree view.

Figure 6-26. DHCP IP Interface

The **DHCP IP Interface** page contains the following fields:

Interface — The specific interface connected to the device. Click the option button next to **Port**, **LAG**, or **VLAN** and select the interface connected to the device.

Host Name — The system name.

Remove — When checked, removes DHCP clients.

Adding DHCP Clients

1. Open the **DHCP IP Interface** page.
2. Click **Add** to display the **Add DHCP IP Interface** page.
3. Complete the information on the page and click **Apply Changes**.

   The DHCP Interface is added, and the device is updated.

Modifying a DHCP IP Interface

1. Open the **DHCP IP Interface** page.
2. Modify the fields.
3. Click **Apply Changes**.

   The entry is modified, and the device is updated.

Deleting a DHCP IP Interface

1. Open the **DHCP IP Interface** page.
2. Click **Show All** to open the **DHCP IP Interface Table** page.
3. Select a DHCP client entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The entry is deleted, and the device is updated.

Defining DHCP IP Interfaces Using CLI Commands

The following table contains the CLI command for defining DHCP clients.

Table 6-19. DHCP IP Interface Commands

CLI Command	Description
`ip address dhcp [hostname` *`hostname`*`]`	To acquire an IP address on an Ethernet interface from the Dynamic Host Configuration Protocol (DHCP)

The following is an example of the CLI command:

```
Console (config-if)# ip address dhcp hostname LA01
```

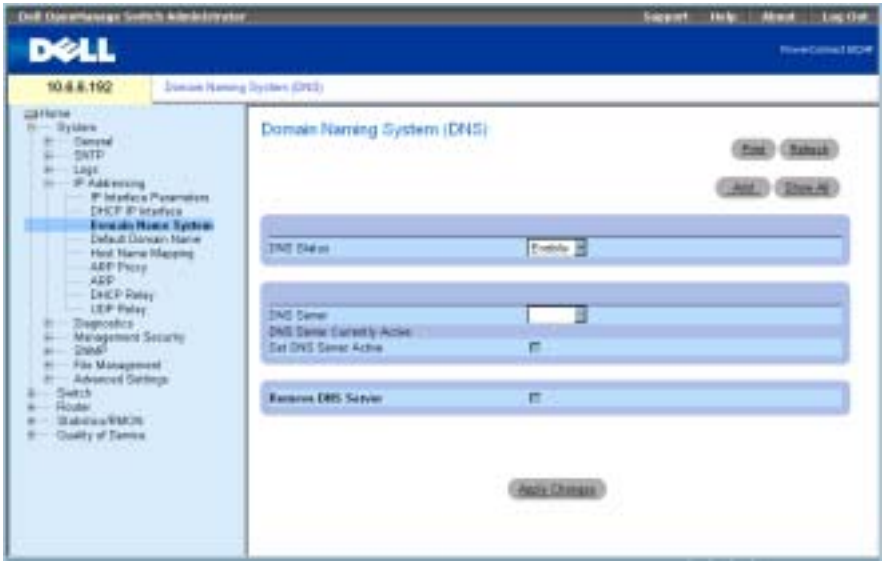
Configuring Domain Name Systems

Domain Name System (DNS) converts user-defined domain names into IP addresses. Each time a domain name is assigned, the DNS service translates the name into a numeric IP address. For example, **www.ipexample.com** is translated to 192.87.56.2. DNS servers maintain domain name databases and their corresponding IP addresses.

The **Domain Naming System (DNS)** page contains fields for enabling and activating specific DNS servers.

To open the **Domain Naming System (DNS)** page, click **System→IP Addressing→Domain Name System** in the tree view.

Figure 6-27. Domain Naming System (DNS)



The **Domain Naming System (DNS)** page contains the following fields:

DNS Status — Enables or disables translating DNS names into IP addresses.

DNS Server — Contains a list of DNS servers. DNS servers are added in the **Add DNS Server** page.

DNS Server Currently Active — The DNS server that is currently active.

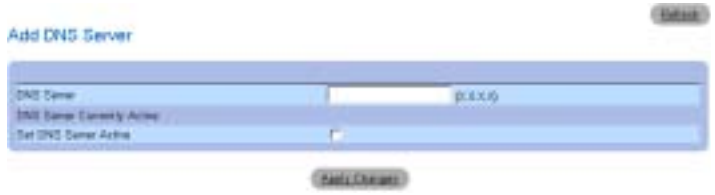
Remove DNS Server — When selected, removes the selected DNS server.

Adding a DNS Server

1. Open the **Domain Naming System (DNS)** page.
2. Click **Add**.

   The **Add DNS Server** page opens:

Figure 6-28. Add DNS Server



The **Add DNS Server** page contains the following fields:

DNS Server — Specifies the DNS server's IP address.

DNS Server Currently Active — Indicates the currently active DNS server.

Set DNS Server Active — Select the check box to define the DNS server as the active DNS server.

3 Define the relevant fields.

4 Click **Apply Changes**.

The new DNS server is defined, and the device is updated.

Displaying the DNS Servers Table

1 Open the **Domain Naming System (DNS)** page.

2 Click **Show All**.

The **DNS Server Table** page opens:

Figure 6-29. DNS Server Table

Removing DNS Servers

1 Open the **Domain Naming System (DNS)** page.

2 Click **Show All**.

3 The **DNS Server Table** page opens.

4 Select a **DNS Server Table** entry.

5 Select the **Remove** check box.

6 Click **Apply Changes**.

The selected DNS server is deleted, and the device is updated.

Configuring DNS Servers Using the CLI Commands

The following table summarizes the CLI commands for configuring DNS servers.

Table 6-20. DNS Server CLI Commands

CLI Command	Description
`ip name-server` *`server-address`*	Sets the available name servers. Up to eight name servers can be set.
`no ip name-server` *`server-address`*	Removes a name server.
`ip domain-name` *`name`*	Defines a default domain name that the software uses to complete unqualified host names. (Range: 1-158 Characters)
`no ip domain-name`	Deletes the default domain name (DNS)
`clear host {`*`name`* `|` *`*`*`}`	Deletes entries from the host name-to-address cache.
`show hosts [`*`name`*`]`	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.
`ip domain-lookup`	Enables DNS system for translating host names to IP addresses.
`no ip domain-lookup`	Disables DNS system for translating host names to IP addresses.

The following is an example of the CLI commands:

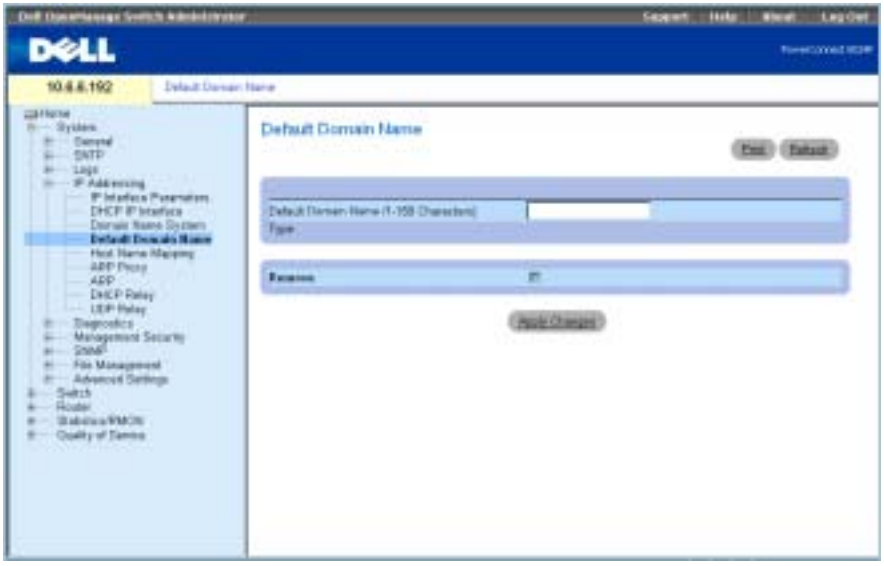
```
Console(config)# ip name-server 176.16.1.18
```

Defining Default Domains

The **Default Domain Name** page provides information for defining default DNS domain names.

To open the **Default Domain Name** page, click **System→IP Addressing→Default Domain Name**.

Figure 6-30. Default Domain Name



The **Default Domain Name** page contains the following fields:

Default Domain Name (1-158 characters) — Contains a user-defined DNS domain name server. When configured, the default domain name is applied to all unqualified host names.

Type — Indicates that the Default Domain Name was created dynamically or statically.

Remove — When selected, removes the default domain name.

Defining DNS Domain Names Using the CLI Commands

The following table summarizes the CLI commands for configuring DNS domain names.

Table 6-21. DNS Domain Name CLI Commands

CLI Command	Description
`ip domain-name` *name*	Defines a default domain name that the software uses to complete unqualified host names.
`no ip domain-name`	Deletes the default domain name (DNS).
`show hosts [`*name*`]`	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

The following is an example of the CLI commands:

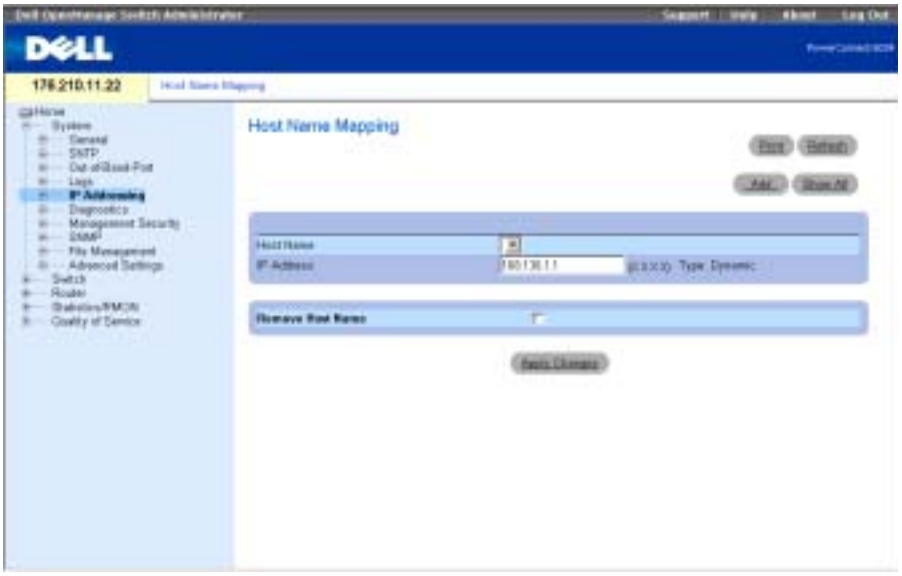
```
Console(config)# ip domain-name dell.com
```

Mapping the Domain Host

The **Host Name Mapping** page provides parameters for assigning an IP address to a static host name. The **Host Name Mapping** page provides one IP address per host.

To open the **Host Name Mapping** page, click **System→IP Addressing→Host Name Mapping.**

Figure 6-31. Host Name Mapping



The **Host Name Mapping** page contains the following fields:

Host Name — Contains a list of host names. Host names are defined in the **Add Host Name Mapping** page. Each host provides one IP address.

IP Address (X.X.X.X) — Provides an IP address that is assigned to the specified host name.

Type — The IP address type. The possible field values are:

Dynamic — The IP address was created dynamically.

Static — The IP address is a static IP address.

Remove Host Name — When checked, removes the DNS host mapping.

Adding Host Domain Names

1. Open the **Host Name Mapping** page.
2. Click **Add**.

   The **Add Host Name Mapping** page opens:

Figure 6-32. Add Host Name Mapping

3 Define the relevant fields.

4 Click **Apply Changes**.

The IP address is mapped to the host name, and the device is updated.

Displaying the Host Names Mapping Table

1 Open the **Host Name Mapping** page.

2 Click **Show All**.

The **Host Name Mapping Table** opens:

Figure 6-33. Host Name Mapping Table

Removing a Host Name from IP Address Mapping

1 Open the **Host Name Mapping** page.

2 Click **Show All**.

The **Host Name Mapping Table** opens.

3 Select a **Host Name Mapping Table** entry.

4 Check the **Remove** check box.

5 Click **Apply Changes**.

The **Host Name Mapping Table** entry is deleted, and the device is updated.

Mapping an IP Address to Domain Host Names Using the CLI Commands

The following table summarizes the equivalent CLI commands for mapping domain host names to IP addresses.

Table 6-22. Domain Host Name CLI Commands

CLI Command	Description
`ip host` *name address*	Defines the static host name-to-address mapping in the host cache.
`no ip host` *name*	Removes the name-to-address mapping.
`clear host {`*name* `|` *`*`*`}`	Deletes entries from the host name-to-address cache.
`clear host dhcp {`*name* `|` *`*`*`}`	Deletes entries from the host name-to-address cache received from the Dynamic Host Configuration Protocol (DHCP).
`show hosts [`*name*`]`	Displays the default domain name, list of name server hosts, the static and the cached list of host names and addresses.

The following is an example of the CLI commands:

```
Console(config)# ip host accounting.abc.com 176.10.23.1
```

Enabling ARP Proxy

Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. The **ARP Proxy** page allows network managers to enable ARP Proxy on the switch.

To open the **ARP Proxy** page, click **System→IP Addressing→ARP Proxy** in the tree view.

Figure 6-34. ARP Proxy

The **ARP Proxy** field enables the device to respond to ARP requests for located nodes. If disabled, the device responds with its own MAC address

Enabling ARP

1. Open the **ARP Proxy** page.
2. Select **Enabled** in the **ARP Proxy** field.
3. Click **Apply Changes**.

   The ARP Proxy is enabled on the device.

Enabling ARP Proxy Using CLI Commands

The following table contains the CLI commands for enabling the ARP Proxy.

Table 6-23. ARP Proxy CLI Commands

CLI Command	Description
`ip proxy-arp`	Enables ARP proxy
`no ip proxy-arp`	Disables ARP proxy

The following is an example of the CLI commands:

```
Console (config)# ip proxy-arp
```

Defining ARP Settings

Use the **ARP Settings** page to define ARP parameters for an IP interface. The ARP table is used to maintain a correlation between each MAC address and its corresponding IP address. The ARP table can be filled in statically by the user. When a static ARP entry is defined, a permanent entry is put in the table, which the system uses to translate IP addresses to MAC addresses.

To open the **ARP Settings** page, click **System→IP Addressing→ARP** in the tree view.

Figure 6-35. ARP Settings

The **ARP Settings** page contains the following fields:

Global Settings — Select this option of activate the fields for ARP global settings.

ARP Entry Age Out (0- 40000000) — For all devices, the amount of time (seconds) that pass between ARP requests about an ARP table entry. After this period, the entry is deleted from the table. The range is 0 - 4000000, where zero indicates that entries are never cleared from the cache.

Clear ARP Table Entries—The type of ARP entries that are cleared on all devices. The possible values are:

None — ARP entries are not cleared.

All — All ARP entries are cleared.

Dynamic — Only dynamic ARP entries are cleared.

Static — Only static ARP entries are cleared.

ARP Entry — Select this option to activate the fields for ARP settings on a single device.

Interface — The interface number of the port, LAG, or VLAN that is connected to the device.

IP Address — The station IP address, which is associated with the MAC address filled in below.

MAC Address — The station MAC address, which is associated in the ARP table with the IP address.

Status — The ARP Table entry status. Possible field values are:

Other — The ARP entry was not dynamically learned and is not a static entry.

Invalid — The ARP entry is invalid.

Dynamic — The ARP entry was learned dynamically.

Static — The ARP entry is a static entry.

Remove ARP Entry — When checked, removes an ARP entry.

Adding an ARP Table Entry

1. Open the **ARP Settings** page.
2. Click **Add** to display the **Add ARP Entry** page.

Figure 6-36. Add ARP Entry Page

3 Select an interface and complete the fields in the page.

4 Click **Apply Changes**.

The ARP Table static entry is added, and the device is updated.

Modifying an ARP Table Entry

1 Open the **ARP Settings** page.

2 Select a table entry.

3 Modify the required fields for a given interface.

4 Click **Apply Changes**.

The **ARP Table** static entry is modified, and the device is updated.

Deleting an ARP Table Entry

1 Open the **ARP Settings** page.

2 Click **Show All** to display the **ARP Table** page.

3 Select a table entry.

4 Check **Remove**.

5 Click **Apply Changes**.

The table entry is deleted, and the device is updated.

Configuring ARP Using the CLI Commands

The following table contains the CLI commands for configuring the ARP.

Table 6-24. ARP Settings CLI Commands

CLI Command	Description
`arp` *`ip_addr hw_addr`* `{ethernet interface-number |` *`vlan vlan-id`* `| port-channel number | out-of-band-eth oob-interface}`	To add a permanent entry in the Address Resolution Protocol (ARP) cache.
`arp timeout`	To configure how long an entry remains in the ARP cache.
`show arp`	To display the entries in the ARP table.

The following is an example of the CLI commands:

```
Console (config)# arp timeout 5

Console (config)# arp 10.1.1.1 0060.704C.73FF ethernet g5

Console# show arp

Interface   IP Address   HW Address       Status

----------  ----------   -----------      -------


   g20      10.1.1.1     0060.704c.73ff   dynamic
```

Defining DHCP Relay Parameters

Use the **DHCP Relay** page to provide information for establishing a DHCP configuration with multiple DHCP servers to ensure redundancy. IP Addresses are controlled and distributed one-by-one to avoid overloading the device.

To open the **DHCP Relay** page, click **System→IP Addressing→DHCP Relay** in the tree view.

Figure 6-37. DHCP Relay

Enabling DHCP Relay

1. Open the **DHCP Relay** page.
2. Select **Enable** from the **DHCP Relay** drop-down menu.
3. Click **Apply Changes**.

   The **DHCP Relay** entry is added to the **DHCP Relay TTable**.

Adding a DHCP Relay Entry

1. Open the **DHCP Relay** page.
2. Click **Add** to open the **Add DHCP Server** page.
3. Enter a value for **New DHCP Server**.

   DHCP servers act as a DHCP relay if this parameter is not equal to 0.0.0.0. DHCP requests are relayed only if their SEC field is greater or equal to the threshold value. This allows local DHCP Servers to answer first.
4. Click **Apply Changes**.

   The DHCP server is added to the **DHCP Relay Table.**

Deleting a DHCP Relay Table Entry

1. Open the **DHCP Relay** page.
2. Click **Show All** to open the **DHCP Servers Table** page.
3. Select a **DHCP Server** and check **Remove**.
4. Click **Apply Changes**.

   The entry is deleted, and the device is updated.

Defining DHCP Relay Servers Using CLI Commands

The following table contains the CLI commands for defining DHCP Relay servers.

Table 6-25. DHCP Relay Server CLI Commands

CLI Command	Description
`ip dhcp relay enable`	Enables Dynamic Host Configuration Protocol (DHCP) relay features on the router.
`ip dhcp relay address` *`ip_address`*	Sets the DHCP servers available for the DHCP relay.

The following is an example of a CLI command to enable DHCP relay service:

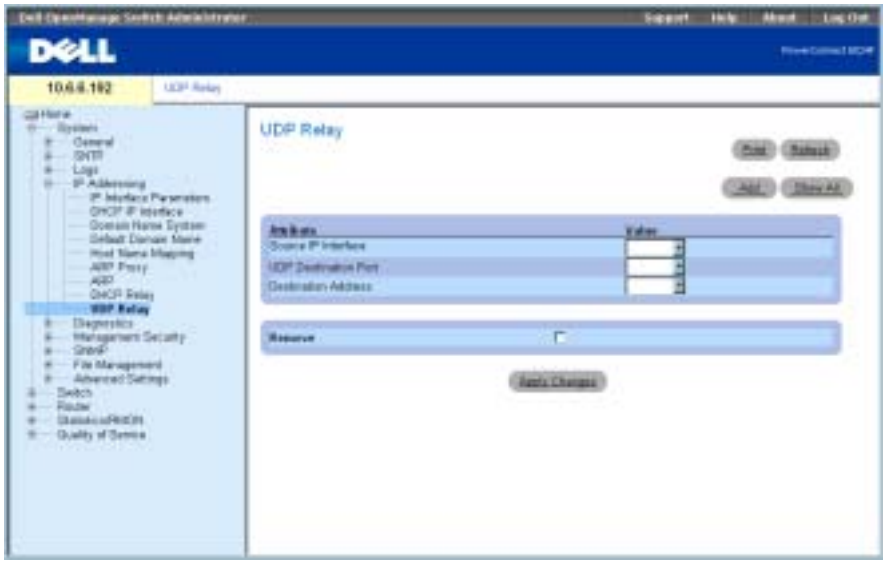
```
Console (config)# ip dhcp relay enable
```

Configuring UDP Relay

UDP Relay allows UDP packets to reach other networks. This feature enables browsing from workstations to servers on different networks.

To open the **UDP Relay** page, click **System→IP Addressing→UDP Relay** in the tree view.

Figure 6-38. UDP Relay



The **UDP Relay** page contains the following fields:

Source IP Interface — The input IP interface that relays UDP packets. If this field is 255.255.255.255, UDP packets from all interfaces are relayed. The following address ranges are invalid:

0.0.0.0 to 0.255.255.255.

127.0.0.0 to 127.255.255.255.

UDP Destination Port (1-65535) — The destination UDP port ID number of UDP packets to be relayed. The following table lists UDP Port allocations.

Table 6-26. UDP Port Allocations

UDP Port Number	Acronym	Application
7	Echo	Echo
11	SysStat	Active User

Table 6-26. UDP Port Allocations

UDP Port Number	Acronym	Application
15	NetStat	Netstat
17	Quote	Quote of the day
19	CHARGEN	Character Generator
20	FTP-data	FTP Data
21	FTP	FTP
37	Time	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who is
53	DOMAIN	Domain Name Server
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network Time
137	NetBiosNameService	NT Server to Station Connections
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios	SessionServiceNT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP-trap	Simple Network Management Traps
513	who	Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

Destination Address — The IP interface that receives UDP packet relays. If this field is 0.0.0.0, UDP packets are discarded. If this field is 255.255.255.255, UDP packets are flooded to all IP interfaces.

Adding a UDP Relay Entry

1. Open the **UDP Relay** page.
2. Click **Add** to display the **Add UDP Relay** page.
3. Enter the UDP server IP address in the **UDP Destination Port** field.

4 Click **Apply Changes**.

The DHCP Server is added to the **DHCP Relay Table**.

Modifying a UDP Relay Table Entry

NOTE: If UDP relay is enabled, but no UDP port number is specified, the device by default forwards UDP Broadcast packets for the following services: IEN-116 Name Service (port 42), DNS (port 53), NetBIOS Name Server (port 137), NetBIOS Datagram Server (port 138), TACACS Server (port 49), and Time Service (port 37)

1 Open the **UDP Relay** page.

2 Define the fields.

3 Click **Apply Changes**.

The UDP entry is added to the **UDP Relay Table**, and the device is updated.

Deleting a UDP Relay Table Entry

1 Open the **UDP Relay** page.

2 Click **Show All** to display the **UDP Relay Table** page.

3 Select a UDP Relay server and check **Remove**.

4 Click **Apply Changes**.

The entry is deleted, and the device is updated.

Configuring the UDP Relay Table Using CLI Commands

The following table contains the CLI command for configuring the UDP Relay.

Table 6-27. UDP Relay CLI Commands

CLI Command	Description
`helper-address` *`address`* [*`udp-port-list`*]	Enables forwarding User Datagram Protocol (UDP) Broadcasts received on an interface. This command does not enable forwarding packets using BOOTP/DHCP. To forward packets using BOOTP/DHCP, use the **ip dhcp relay enable**, **ip dhcp relay address** and **show ip dhcp** relay commands. For information about these commands, see **Defining DHCP Relay Parameters**.

The following is an example of the CLI command:

```
Console (config-ip)# helper-address 172.16.9.9 49 53
```

Running Cable Diagnostics

Use the **Diagnostics** page to perform virtual cable tests for copper and fiber optics cables.

To open the **Diagnostics** page, click **System→Diagnostics** in the tree view.

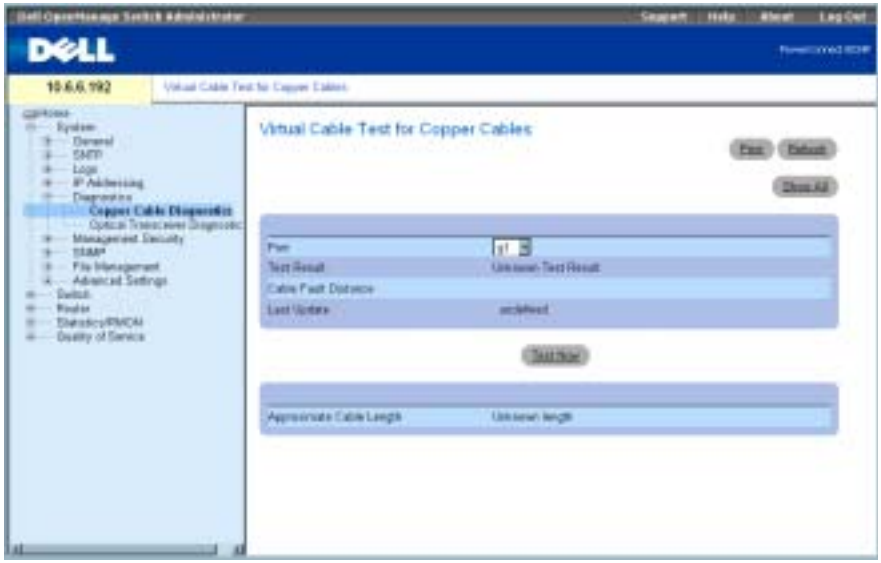
The **Diagnostics** page contains links to diagnostics pages for copper cable and optical transceivers.

Viewing Copper Cable Diagnostics

Use the **Virtual Cable Test for Copper Cables** page to perform tests on copper cables. Cable testing provides information about where errors occurred in the cable, the last time a cable test was performed, and the type of cable error which occurred. The tests use Time Domain Reflectometry (TDR) technology to test the quality and characteristics of a copper cable attached to a port. Cables up to 120 meters long can be tested. Cables are tested when the ports are in the down state, with the exception of the Approximated Cable Length test.

To open the **Virtual Cable Test for Copper Cables** page, click **System→Diagnostics→Copper Cable Diagnostics** in the tree view.

Figure 6-39. Virtual Cable Test for Copper Cables



The **Virtual Cable Test for Copper Cables** page contains the following fields:

Port — The port to which the cable is connected.

Test Result — The cable test results. Possible values are:

No Cable — There is not a cable connected to the port.

Open Cable — The cable is open.

Short Cable — A short has occurred in the cable.

OK — The cable passed the test.

Fiber Cable — A fiber cable is connected to the port.

Cable Fault Distance — The distance from the port where the cable error occurred.

Last Update — The last time the port was tested.

Approximate Cable Length — The approximate cable length. This test can only be performed when the port is up and operating at 1 gbps.

Performing a Cable Test

1. Ensure that both ends of the copper cable are connected to a device.
2. Open the **Virtual Cable Test for Copper Cables** page.
3. Click **Test Now**.

   The copper cable test is performed, and the results are displayed on the **VVirtual Cable Test for Copper Cables** page.

Displaying Virtual Cable Test Results Table

1. Open the **Virtual Cable Test for Copper Cables** page.
2. Click **Show All** to run the tests and display the **Virtual Cable Test Results Table** page.

Performing Copper Cable Tests Using CLI Commands

The following table contains the CLI commands for performing copper cable tests.

Table 6-28. Copper Cable Test CLI Commands

CLI Command	Description
`test copper-port tdr` *`interface`*	Performs VCT tests.
`show copper-port tdr` *`interface`*	Shows results of last VCT tests on ports.
`show copper-port cable-length` *`interface`*	Displays the estimated copper cable length attached to a port.

The following is an example of the CLI commands:

```
Console# show copper-ports cable-length

Port Length [meters]

---- ---------------

g1 < 50

g2 Copper not active

g3 110-140

g4 Fiber
```

NOTE: The cable length returned by the VCT is an approximation in the ranges of up to 50 meters, 50m-80m, 80m-110m, 110m-120m, or more than 120m. The deviation may be up to 20 meters, and cable length measurement will not operate for 10 Mbps links.

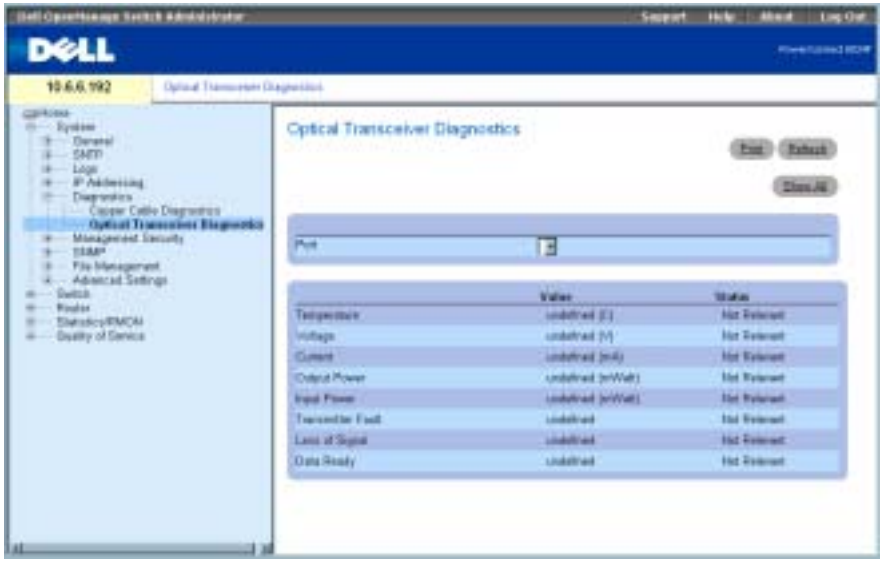
Viewing Optical Transceiver Diagnostics

Use the **Optical Transceiver Diagnostics** page to perform tests on Fiber Optic cables.

To open the **Optical Transceiver Diagnostics** page, click **System→Diagnostics→Optical Transceiver Diagnostics** in the tree view.

NOTE: Optical transceiver diagnostics can be performed only when the link is present.

Figure 6-40. Optical Transceiver Diagnostics



The Optical Transceiver Diagnostics page contains the following fields:

Port — The port IP address on which the cable is tested.

Temperature — The temperature (C) at which the cable is operating.

Voltage — The voltage at which the cable is operating.

Current — The current at which the cable is operating.

Output Power — The rate at which the output power is transmitted.

Input Power — The rate at which the input power is transmitted.

Transmitter Fault — Indicates if a fault occurred during transmission.

Loss of Signal—Indicates if a signal loss occurred in the cable.

Data Ready—Indicates the transceiver has achieved power up and data is ready.

Displaying Optical Transceiver Diagnostics Test Results Table

1. Open the **Optical Transceiver Diagnostics** page.
2. Click **Show All** to run the test and open the **Virtual Cable Test Results Table** page.

Performing Fiber Optic Cable Tests Using CLI Commands

The following table contains the CLI command for performing fiber optic cable tests.

Table 6-29. Fiber Optic Cable Test CLI Command

CLI Command	Description
`show fiber-ports optical-transceiver [interface] [detailed]`	Displays the optical transceiver diagnostics.

The following is an example of the CLI command:

```
console# show fiber-ports optical-transceiver
```

The following columns appear on the screen:

- **Temp** — Internally measured transceiver temperature
- **Voltage** — Internally measured supply voltage
- **Current** — Measured TX bias current
- **Output Power** — Measured TX output power in milliWatts
- **Input Power** — Measured RX received power in milliwatts
- **TX Fault** — Transmitter fault

NOTE: Finisar transceivers do not support the transmitter fault diagnostic testing.

- **LOS** — Loss of signal
- **Data Ready** — Indicates transceiver has archived power up and data is ready
- **N/A** — Not Available, N/S - Not Supported, W - Warning, E - Error

NOTE: Fiber Optic analysis feature works only on SFPs that support the digital diagnostic standard SFF-4872.

Managing Device Security

Use the **Management Security** page to set management security parameters for port, user, and server security.

To open the **Management Security** page, click **System→Management Security** in the tree view.

Defining Access Profiles

Use the **Access Profiles** page to define profiles and rules for accessing the device. You can limit access to management functions to user groups, which are defined by ingress interfaces and source IP address and/or source IP subnets.

Management access can be separately defined for each type of management access method, including, Web (HTTP), Secure web (HTTPS), Telnet, and SNMP.

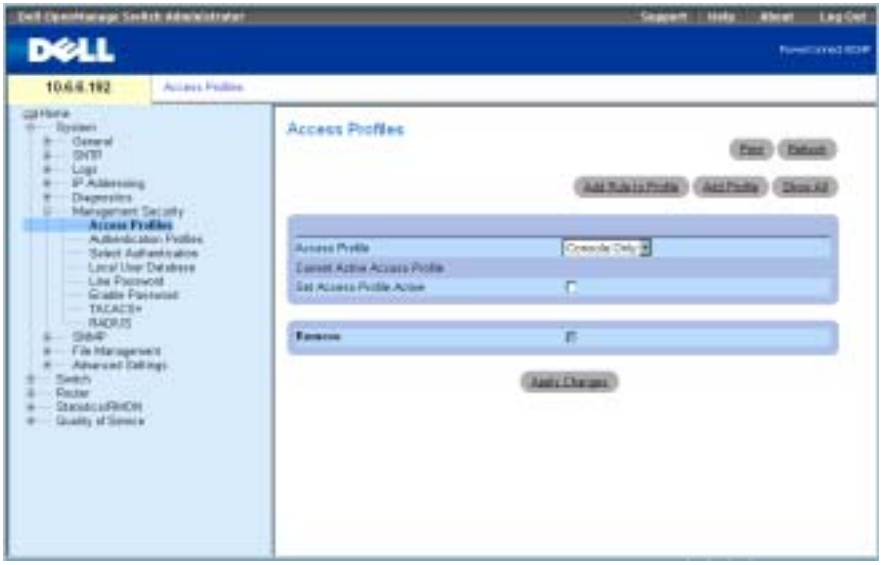
Access to different management methods may differ between user groups. For example, User Group 1 can access the device only via an HTTPs session, while User Group 2 can access the device via both HTTPs and Telnet sessions.

Management Access Lists contain the rules that determine which users can manage the device, and by which methods. Users can also be blocked from accessing the device.

Use the **Access Profiles** page to configure Management Lists and apply them to specific interfaces.

To open the **Access Profiles** page, click **System→Management Security→Access Profiles** in the tree view.

Figure 6-41. Access Profiles



Access Profile — Contains a list of all access profiles. The default value is **Console Only**, to which user-defined access profiles are added. Selecting **Console Only** as the **Access Profile** name disconnects the session, and enables accessing the device from the console only.

Current Active Access Profile — The access profile that is currently active.

Set Access Profile Active — Activates an access profile.

Remove — When checked, removes an access profile from the **Access Profile Name** list.

Adding an Access Profile

1. Open the **Access Profiles** page.
2. Click **Add Profile** to open the **Add an Access Profile** page.

Figure 6-42. Add an Access Profile

The **Add an Access Profile** page contains the following fields:

Access Profile Name — User-defined name for the access profile.

Rule Priority — Indicates the rule priority. When the packet is matched to a rule, user groups are either granted or denied device management access. The rule order is set by defining a rule number within the **Profile Rules** table. The rule number is essential to matching packets to rules, as packets are matched on a first-fit basis. The rule priorities are assigned in the Profile Rules Table.

Management Method — The management method for which the access profile is defined. Users with this access profile can access the device using the management method selected.

Interface — The interface type to which the rule applies. This is an optional field. You can apply this rule to a selected port, LAG, or VLAN by checking the check box and selecting the appropriate option button and interface.

NOTE: Assigning an access profile to an interface implies that access via other interfaces is denied. If an access profile is not assigned to any interface, the device can be accessed by all.

Source IP Address — The interface source IP address for which the rule applies. This is an optional field and indicate that the rule is valid for a subnetwork.

Network Mask — The IP subnetwork mask.

Prefix Length — The number of bits that comprise the source IP address prefix, or the network mask of the source IP address.

Action — Defines whether to permit or deny management access to the defined interface.

3 Enter the profile name in the **Access Profile Name** text box.

4 Complete the fields and click **Apply Changes**.

The new access profile is added, and the device is updated.

Activating an Access Profile

1 Open the **Access Profiles** page.

2 Select an access profile from the list.

3 Check the **Set Access Profile Active** check box.

4 Click **Apply Changes**.

The access profile is enabled for the user.

Adding Rules to an Access Profile

1 Open the **Access Profiles** page.

2 Select an **Access Profile** from the drop-down menu.

This is the profile to which rules are added when the **Add An Access Profile Rule** page is opened.

3 Click **Add Rule to Profile** to open the **Add An Access Profile Rule** page.

Figure 6-43. Add An Access Profile Rule

4 Complete the fields in the dialog and click **Apply Changes**.

The rule is added to the access profile, and the device is updated.

Removing a Rule

1 Open the **Access Profiles** page.

2 Click **Show All** to display the **Profile Rules Table** page.

3 Select a rule.

4 Check the **Remove** check box and click **Apply Changes**.

The rule is deleted, and the device is updated.

Defining Access Profiles Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring access profiles.

Table 6-30. Access Profile CLI Commands

CLI Command	Description
`management access-list` *name* **NOTE:** Enclose *name* in double quotes if it contains spaces. For example, "workgroup 1"	Defines an access-list for management, and enters the access-list context for configuration.
`permit [ethernet` *interface-number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`]`	Sets port permitting conditions for the management access list.
`permit ip-source` *ip-address* `[mask` *mask* / *prefix-length*`] [ethernet` *interface-number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`]`	Sets port permitting conditions for the management access list, and the selected management method.
`deny [ethernet` *interface-number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`]`	Sets port denying conditions for the management access list, and the selected management method.
`deny ip-source` *ip-address* `[mask` *mask* / *prefix-length*`] [ethernet` *interface-number* `| vlan` *vlan-id* `| port-channel` *number*`] [service` *service*`]`	Sets port denying conditions for the management access list, and the selected management method.
`management access-class {console-only |` *name*`}`	Defines which access-list is used as the active management connections.
`show management access-list [`*name*`]`	Displays the active management access-lists.
`show management access-class`	Displays information about management access-class.

The following is an example of the CLI commands:

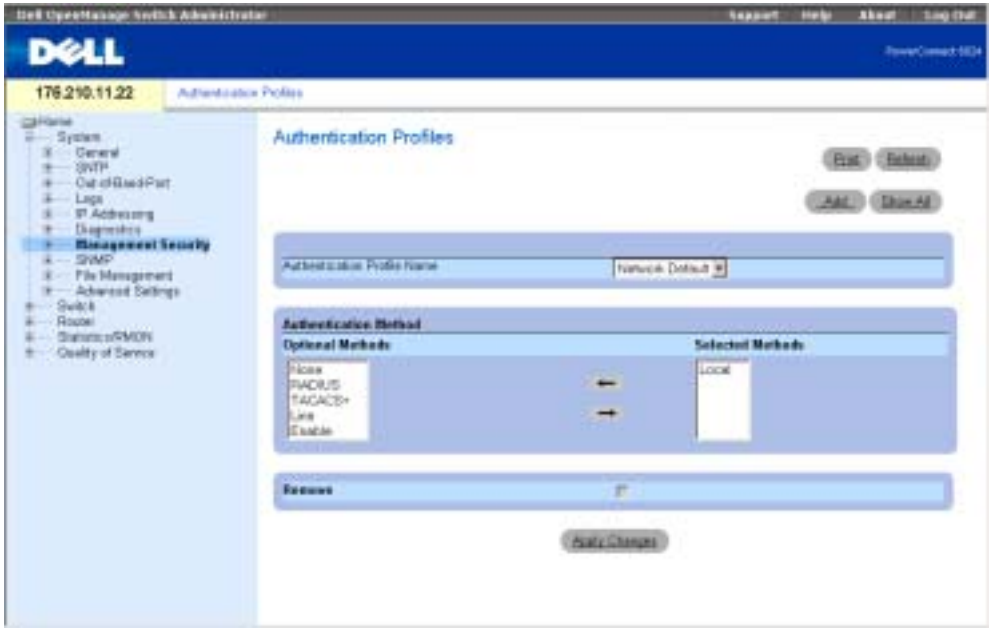
```
Console (config)# management access-list mlist
Console (config-macl)# permit ethernet g1
Console (config-macl)# permit ethernet g9
Console (config-macl)# exit
Console# show management access-class
Management access-class is enabled, using access list mlist
```

Defining Authentication Profiles

User authentication occurs locally and on an external server. Use the **Authentication Profiles** page to select the user authentication method on the device.

To open the **Authentication Profiles** page, click **System→Management Security→Authentication Profiles** in the tree view.

Figure 6-44. Authentication Profiles



The **Authentication Profiles** page contains the following fields:

Authentication Profile Name — User-defined authentication profile lists to which user-defined authentication profiles are added. The defaults are **Network Default** and **Console Default**.

Optional Methods — User authentication methods. Possible options are:

None — No user authentication occurs.

Local — User authentication occurs at the device level; the device checks the user name and password for authentication.

RADIUS — User authentication occurs at the RADIUS server. For more information about RADIUS servers, see "Configuring RADIUS Settings."

TACACS+ — User authentication occurs at the TACACS+ server. For more information about TACACS+ servers, see "Configuring TACACS+ Settings."

Line — The line password is used for user authentication.

Enable — The enable password is used for authentication.

NOTE: User authentication occurs in the order the methods are selected. If an error occurs during the authentication, the next selected method is used. For example, if both the **Local** and **RADIUS** options are selected, the user is authenticated first locally and then via an external server.

Selected Methods — The selected authentication method.

Adding an Authentication Profile

1. Open the **Authentication Profiles** page.
2. Click **Add** to display the **Add Authentication Profile** page.
3. Enter the profile name of 1-12 characters in the **Profile Name** field.

NOTE: The profile name should not include spaces.

4. Click **Apply Changes**.

   Sessions are assigned an authentication profile.

Selecting an Authentication Method

1. Open the **Authentication Profiles** page.
2. Select an element from the list in the **Authentication Profile Name** field.
3. Select an **Optional Methods** value by using the arrows.
4. Click **Apply Changes**.

   The user authentication profile is updated to the device.

Removing an Authentication Profiles Entry

1. Open the **Authentication Profiles** page.
2. Click **Show All**.

   The **Authentication Profiles** Table opens.

3. Check the **Remove** check box next to the profile to be removed.

4 Click **Apply Changes**.

The entry is removed.

Configuring an Authentication Profile Using CLI Commands

The following table summarizes the equivalent CLI commands for defining authentication profiles.

Table 6-31. Authentication Profile CLI Commands

CLI Command	Description
`aaa authentication login {default | list-name} method1 [method2...]`	Configures login authentication.
`no aaa authentication login {default | list-name}`	Removes a login authentication profile.
`show authentication methods`	Displays information about the authentication methods.

The following is an example of the CLI commands:

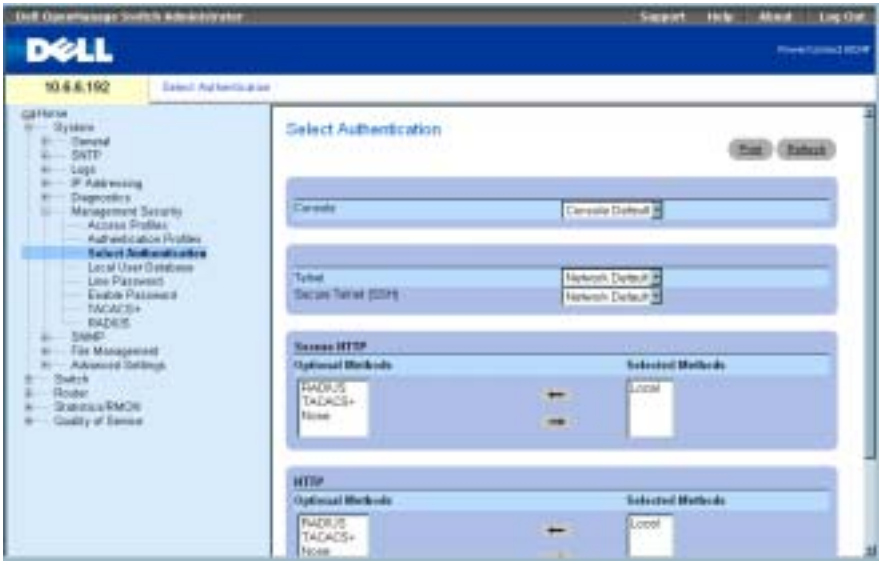
```
Console (config)# aaa authentication login default radius local
enable none

Console (config)# no aaa authentication login default
```

Selecting Authentication Profiles

After authentication profiles are defined, they can be applied to management access methods. For example, console users can be authenticated by Authentication Profile List 1, while Telnet users are authenticated by Authentication Method List 2.

To open the **Select Authentication** page, click **System→Management Security→Select Authentication** in the tree view.

Figure 6-45. Select Authentication



The **Select Authentication** page contains the following fields:

Console — Authentication profiles used to authenticate console users.

Telnet — Authentication profiles used to authenticate Telnet users.

Secure Telnet (SSH) — Authentication profiles used to authenticate Secure Shell (SSH) users. SSH provides clients secure and encrypted remote connections to a device.

HTTP and **Secure HTTP** — Authentication method used for HTTP access and Secure HTTP access, respectively. Possible field values are:

None — No authentication method is used for access.

Local — Authentication occurs locally.

RADIUS — Authentication occurs at the RADIUS server.

TACACS+ — Authentication occurs at the TACACS+ server.

Local, None — Authentication first occurs locally. If authentication cannot be verified, no authentication method is used.

RADIUS, None — Authentication first occurs at the RADIUS server. If authentication cannot be verified, no authentication method is used.

TACACS+, None — Authentication first occurs at the TACACS+ server. If authentication cannot be verified, no authentication method is used.

Local, RADIUS — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is blocked.

Local, TACACS+ — Authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is blocked.

RADIUS, Local — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.

TACACS+, Local — Authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is blocked.

Local, RADIUS, None — Authentication first occurs locally. If authentication cannot be verified locally, the RADIUS server authenticates the management method. If the RADIUS server cannot authenticate the management method, the session is permitted.

RADIUS, Local, None — Authentication first occurs at the RADIUS server. If authentication cannot be verified at the RADIUS server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

Local, TACACS+, None — Authentication first occurs locally. If authentication cannot be verified locally, the TACACS+ server authenticates the management method. If the TACACS+ server cannot authenticate the management method, the session is permitted.

TACACS+, Local, None — Authentication first occurs at the TACACS+ server. If authentication cannot be verified at the TACACS+ server, the session is authenticated locally. If the session cannot be authenticated locally, the session is permitted.

Applying an Authentication Method List to Console Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Console** field.
3. Click **Apply Changes**.

   Console sessions are assigned an authentication method List.

Applying an Authentication Profile to Telnet Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Telnet** field.
3. Click **Apply Changes**.

   Console sessions are assigned authentication profiles.

Applying an Authentication Profile to Secure Telnet (SSH) Sessions

1. Open the **Select Authentication** page.
2. Select an authentication profile in the **Secure Telnet (SSH)** field.
3. Click **Apply Changes**.

   Secure Telnet (SSH) sessions are assigned authentication profiles.

Assigning HTTP Sessions an Authentication Sequence

1. Open the **Select Authentication** page.
2. Under **HTTP**, select an authentication method in the **Optional Methods** field and click the right arrow button.

   The selected authentication method moves to the **Selected Methods** field.
3. Repeat until the desired authentication sequence is displayed in the **Selected Methods** field.
4. Click **Apply Changes**.

   HTTP sessions are assigned the authentication sequence.

Assigning Secure HTTP Sessions an Authentication Sequence

1. Open the **Select Authentication** page.
2. Under **Secure HTTP**, select an authentication method in the **Optional Methods** field and click the right arrow button.

   The selected authentication method moves to the **Selected Methods** field.
3. Repeat until the desired authentication sequence is displayed in the **Selected Methods** field.
4. Click **Apply Changes**.

   Secure HTTP sessions are assigned the authentication sequence.

Assigning Access Methods Authentication Profiles or Sequences

The following table contains the CLI commands for assigning access methods, authentication method lists, or sequences.

Table 6-32. Access Methods CLI Commands

CLI Command	Description
`enable authentication {default | list-name}`	Specifies authentication method list when the user accesses higher privilege levels in remote telnet or console.
`login authentication {default | list-name}`	Specifies login authentication method list for remote telnet or console.

Table 6-32. Access Methods CLI Commands

CLI Command	Description
`ip http authentication method1 [method2...]`	Specifies authentication methods for http server users.
`ip https authentication method1 [method2...]`	Specifies authentication methods for https server users.
`show authentication methods`	Displays information about the authentication methods.

The following is an example of the CLI commands:

```
Console# show authentication methods

Login Authentication Method Lists

---------------------------------

Default             : Local


Enable  Authentication Method Lists

---------------------------------

Console_Default     : Enable   None

Network_Default     : Enable


Line           Login Method List         Enable Method List

-------        -----------------         -------------------

Console        Default                   Default

Telnet         Default                   Default

SSH            Default                   Default


http                : Local

https               : Local
```

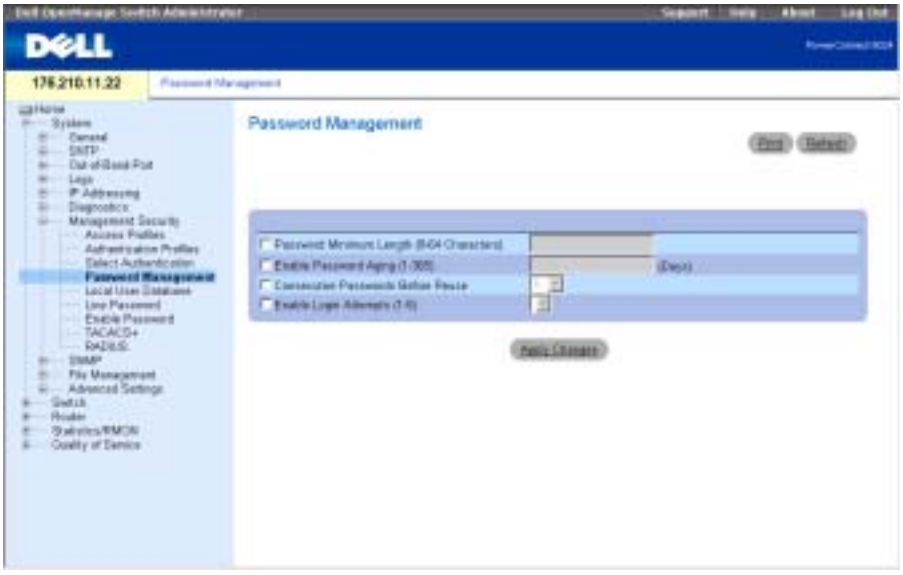
Managing Passwords

Password management provides increased network security and improved password control. Passwords for SSH, Telnet, HTTP, HTTPS, and SNMP access are assigned security features, including:

- Defining minimum password lengths
- Password expiration
- Preventing frequent password reuse
- Locking out users out after failed login attempts

To open the **Password Management** page, click To open the **Password Management** page, click **System→Management Security→Password Management** in the tree view.

Figure 6-46. Password Management



The **Password Management** page contains the following fields:

Password Minimum Length (8-64 Characters)— Indicates the minimum password length, when checked. For example, the administrator can define that all line passwords must have a minimum of 10 characters.

Enable Password Aging (1-365)— Indicates the amount of time that elapses before a password is aged out, when checked. The field value is between 1-365 days.

Consecutive Passwords Before Reuse— Indicates the amount of times a password is changed, before the password can be reused. The possible field values are 1 - 10.

NOTE: The user is notified to change the password prior to expiry. The Web users do not see this notification.

Enable Login Attempts (1-5)— When selected, enables locking a user out of the device when a faulty password is used a defined number of times. For example, if the number of login attempts has been defined as five and the user attempts to log on five times with an incorrect password, the device locks the user out on the sixth attempt. The field range is 1-5 attempts.

Defining Password Constraints

1. Open the **Password Management** page.
2. Define the relevant fields.
3. Click **Apply Changes**.

   The password constraints are defined, and the device is updated.

Defining Password Constraints Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring passwords on the **Password Management** page.

Table 6-33. Password Management CLI Commands

CLI Command	Description
`password min-length` *`length`*	Defines minimum length required for passwords.
`passwords aging` *`days`*	Defines the expiration time of passwords in the local database.
`passwords history` *`number`*	Defines the number of required password changes before a password in the local database can be re-used
`passwords lock-out` *`number`*	Locks a user account after a specified number of failed login attempts.
`show password configuration`	Displays information about password management.

The following is an example of the CLI commands:

```
Console (config)# password min-length 8
Console (config)# password aging 120
Console (config)# passwords history 2
Console (config)# passwords lock-out 3
Console (config)# exit
```

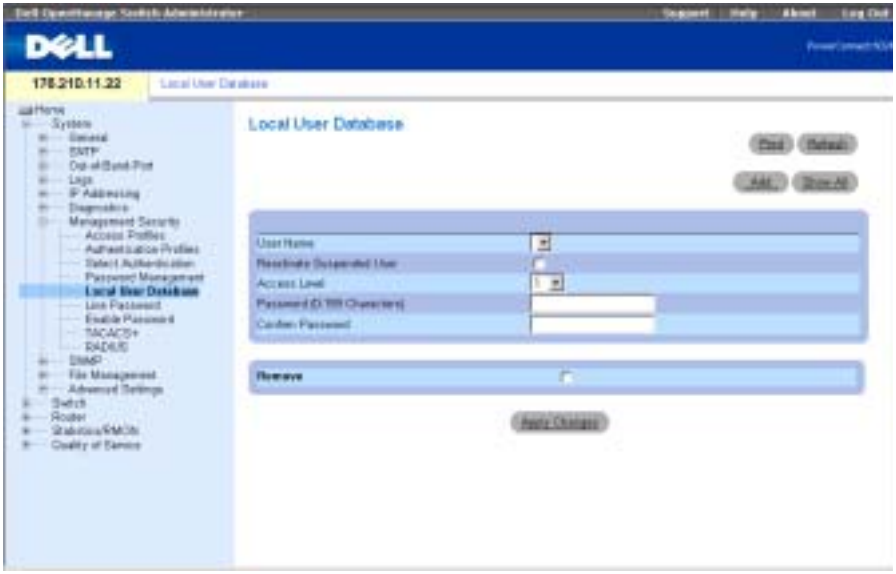
```
Console# show passwords configuration
Minimal  length: 8
Aging: 120 days
History: 2
Lock-out: Disabled
```

Defining the Local User Databases

Use the **Local User Database** page to define passwords, access rights for users and reactivate users whose accounts have been suspended.

To open the **Local User Database** page, click **System→Management Security→Local User Database** in the tree view.

Figure 6-47. Local User Database



The **Local User Database** page contains the following fields:

User Name — List of users.

Reactivated Suspended User — Select to reactivate the specified user's access rights. Access rights can be suspended after unsuccessfully attempting to login.

Access Level (1-15) — User access level. The lowest user access level is **1** and **15** is the highest user access level.

Password — User-defined password.

Confirm Password — Confirms the user-defined password.

Remove — When selected, removes users from the **User Name** list.

Assigning Access Rights to a User

1. Open the **Local User Database** page.
2. Select a user in the **User Name** field.
3. Define the fields.
4. Click **Apply Changes**.

   The user's access rights and passwords are defined, and the device is updated.

Adding a User to the Local User Database

1. Open the **Local User Database** page.
2. Click **Add** to display the **Add User** page.
3. Complete the fields.
4. Click **Apply Changes**.

   The new user is defined, and the device is updated.

NOTE: You can define as many as 30 users on the device.

Reactivating a Suspended User

1. Open the **Local User Database** page.
2. Click **Show All** to open the **Local User Table** page.
3. Select a **User Name** entry.
4. Select the **Reactivate Suspended User** check box.
5. Click **Apply Changes**.

   The user 's access rights are reactivated, and the device is updated.

Deleting Users From the Local User Database

1. Open the **Local User Database** page.
2. Click **Show All** to open the **Local User Table**.
3. Select a **User Name**.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The user is deleted, and the device is updated.

Assigning Users Using CLI Commands

The following table summarizes the equivalent CLI commands for viewing fields displayed on the **Local User Database** page.

Table 6-34. Local User Database CLI Commands

CLI Command	Description
`username` *name* `[password` *password*`] [privilege` *level*`] [encrypted]`	Establishes a username-based authentication system.
`set username` *name* `active`	Reactivates a locked user account.

The following is an example of the CLI commands:

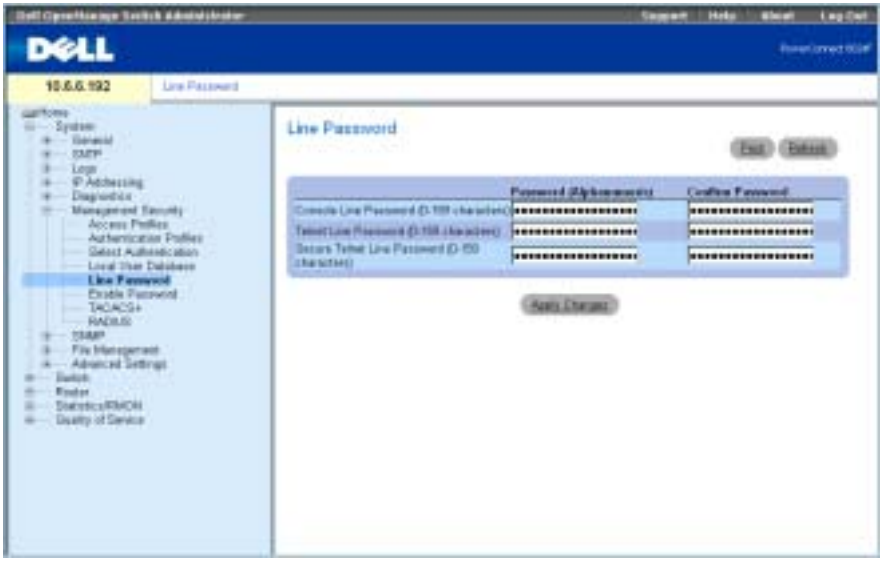
```
console (config)#username bob password lee privilege 15
console# set username bob active
```

Defining Line Passwords

Use the **Line Password** page to define line passwords for management methods.

To open the **Line Password** page, click **System > Management Security > Line Password** in the tree view.

Figure 6-48. Line Password



The **Line Password** page contains the following fields:

Line Password for Console/Telnet/Secure Telnet — The line password for accessing the device via a console, Telnet, or Secure Telnet session.

Confirm Password — Confirms the new line password. The password appears in the ***** format.

Defining Line Passwords

1. Open the **Line Password** page.
2. Define the **Line Password** field for the type of session you use to connect to the device.
3. Click **Apply Changes**.

   The line password for the type of session is defined, and the device is updated.

Assigning Line Passwords Using CLI Commands

The following table summarizes the equivalent CLI commands for defining line passwords.

Table 6-35. Line Password CLI Commands

CLI Command	Description
`password` *`password`* `[encrypted]`	Specifies a password on a line.

The following is an example of the CLI commands:

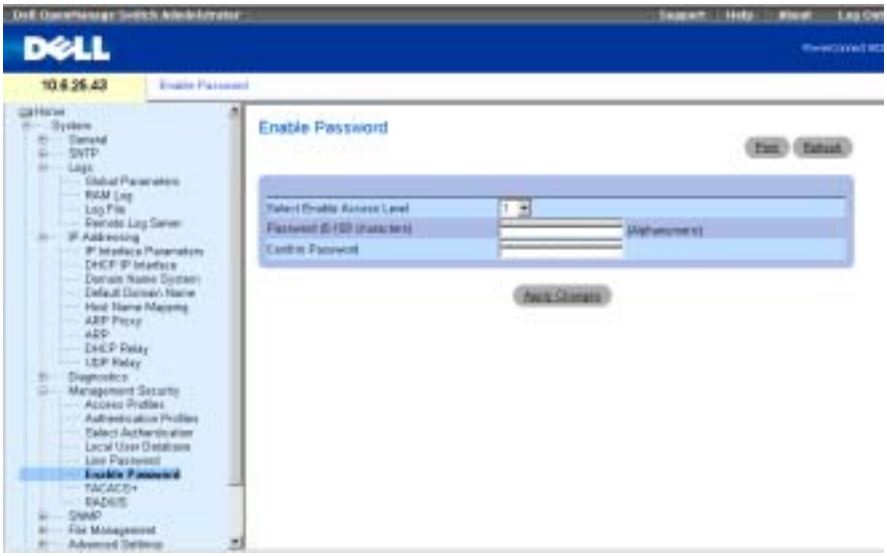
```
Console (config-line)# password ****
```

Defining Enable Password

The **Modify Enable Password** page sets a local password to control access to different privilege levels (1-15).

To open the **Modify Enable Password** page, click **System→Management Security→Enable Password** in the tree view.

Figure 6-49. Modify Enable Password



The **Modify Enable Password** page contains the following fields:

Select Enable Access Level — Access level associated with the enable password. Possible field values are 1-15.

Password — The current enable password.

Confirm Password — Confirms the new enable password. The password appears in the ***** format.

Defining a New Enable Password

1. Open the **Modify Enable Password** page.
2. Complete the fields in the dialog.

3 Click **Apply Changes**.

The new password is defined, and the device is updated.

Assigning Enable Passwords Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields displayed in the **Modify Enable Password** page.

Table 6-36. Enable Password CLI Commands

CLI Command	Description
`enable password [level` *`level`*`] password [encrypted]`	Sets a local password to control access to user and privilege levels.
`show users accounts`	Displays information about the local user database.

```
The following is an example of the CLI commands:
Console (config)# enable password level 15 dell
Console# show users accounts
Username    Privilege
---------   ---------
Bob           15
Jim           15
Dell         1515
```

Configuring TACACS+ Settings

The device provide Terminal Access Controller Access Control System (TACACS+) client support. TACACS+ provides centralized security for validation of users accessing the device.

TACACS+ provides a centralized user management system, while still retaining consistency with RADIUS and other authentication processes. TACACS+ provides the following services:

- **Authentication** — Provides authentication during login and via user names and user-defined passwords.
- **Authorization** — Performed at login. Once the authentication session is completed, an authorization session starts using the authenticated user name. The TACACS+ server checks the user privileges.

The TACACS+ protocol ensures network integrity through encrypted protocol exchanges between the device and TACACS+ server.

The **TACACS+ Settings** page contains both user-defined and the default TACACS+ settings for the inband management port.

To open the **TACACS+ Settings** page, click **System→Management Security→TACACS+** in the tree view.

Figure 6-50. TACACS+ Settings

The **TACACS+ Settings** page contains the following fields:

Host IP Address — Specifies the TACACS+ Server IP address.

Priority (0-65535) — Specifies the order in which the TACACS+ servers are used. The default is 0.

Source IP Address — The device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — Defines the authentication and encryption key for TACACS+ communications between the device and the TACACS+ server. This key must match the encryption used on the TACACS+ server.

Authentication Port (0-65535) — The port number through which the TACACS+ session occurs. The default is port 49.

Timeout for Reply (1-30) — The amount of time that passes before the connection between the device and the TACACS+ server times out. The field range is 1-30 seconds.

Status — The connection status between the device and the TACACS+ server. The possible field values are:

Connected — There is currently a connection between the device and the TACACS+ server.

Not Connected — There is not currently a connection between the device and the TACACS+ server.

Single Connection — Maintains a single open connection between the device and the TACACS+ server when selected

The TACACS+ default parameters are user-defined defaults. The default settings are applied to newly defined TACACS+ servers. If default values are not defined, the system defaults are applied to the new TACACS+ servers. The following are the TACACS+ defaults:

Source IP Address — The default device source IP address used for the TACACS+ session between the device and the TACACS+ server.

Key String (0-128 Characters) — The default authentication and encryption key for TACACS+ communication between the device and the TACACS+ server.

Timeout for Reply (1-30) — The default time that passes before the connection between the device and the TACACS+ times out.

NOTE: The aforementioned defaults also apply to the **OOB TACACS+ Settings** page (**System→Out-of-Band-Port→TACACS+**).

Defining TACACS+ Parameters

1. Open the **TACACS+ Settings** page.
2. Define the fields.
3. Click **Apply Changes**.

   The TACACS+ settings are updated to the device.

Adding a TACACS+ Server

1. Open the **TACACS+ Settings** page.
2. Click **Add**.

   The **Add TACACS+ Host** page opens.
3. Define the fields.
4. Click **Apply Changes**.

   The TACACS+ server is added, and the device is updated.

Deleting a TACACS+ Server from the TACACS+ Servers List

1. Open the **TACACS+ Settings** page.
2. Click **Show All**.

   The **TACACS+ Table** opens.
3. Select a **TACACS+ Table** entry.
4. Select the **Remove** check box.
5. Click **Apply Changes**.

   The TACACS+ server is removed, and the device is updated.

Defining TACACS+ Servers Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring fields displayed in the **TACACS+ Settings** page.

Table 6-37. TACACS+ Settings CLI Commands

CLI Command	Description
`tacacs-server host {ip-address | hostname} [single-connection] [port port-number] [timeout timeout] [key key-string] [source source] [priority priority]`	Specifies a TACACS+ server host.
`no tacacs-server host {ip-address | hostname}`	Deletes a specified TACACS+ server host.
`tacacs-server key [key-string]`	Specifies the authentication and encryption key used for all TACAS communication between the router and the TACACS+ server. This key must match the encryption used on the TACACS daemon. (Range:0-128 characters)
`no tacacs-server key`	Returns to the default.
`tacacs-server timeout timeout`	Specifies the timeout value in seconds. (Range: 1-30)
`no tacacs-server timeout`	Returns to the default.
`tacacs-server source-ip ip-address`	Specifies the source IP address. (Range: Valid IP address)
`no tacacs-server source-ip ip-address`	Returns to the default.

Table 6-37. TACACS+ Settings CLI Commands

CLI Command	Description
`show tacacs+ [ip-address]`	Displays configuration and statistics for a TACACS+ server.

The following is an example of the CLI commands:

```
Console(config)# tacacs-server host 171.16.8.1 port 49 key abc
Console(config)# end
Console# show tacacs

Device Configuration
--------------------
IP address    Status     Port  Single      TimeOut  Source   Priority
                               Connection           IP
-----------   ---------  ----  ----------  -------  ------   --------
171.16.8.1    Not        49    No          Global   Global   0
              Connected

OOB Host Configuration
IP address    Status     Port  Single      TimeOut  Source   Priority
                               Connection           IP
-----------   ---------  ----  ----------  -------  ------   --------
No TACACS server is configured.

Device Configuration
--------------------
Source IP: 0.0.0.0

OOB host Configuration
----------------------
Source IP : 0.0.0.0
```

Configuring RADIUS Settings

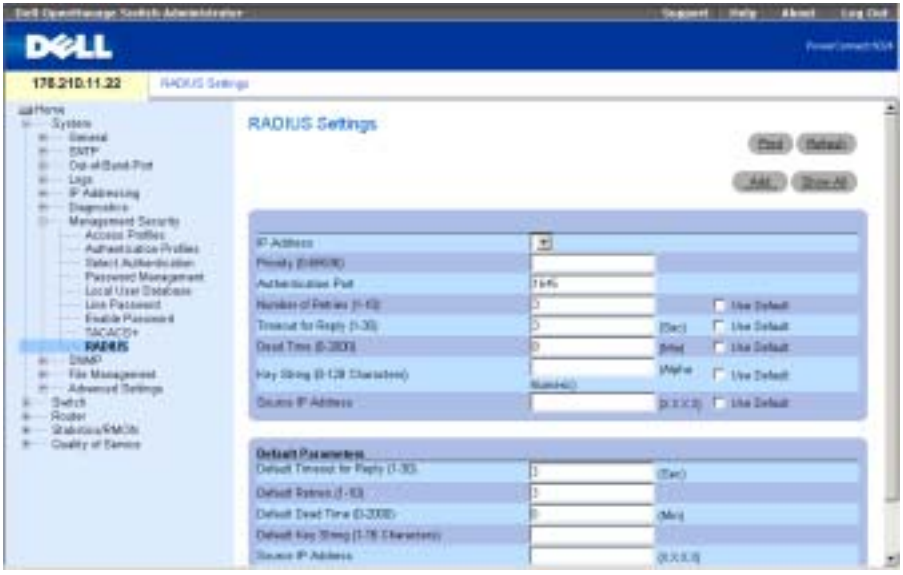
Remote Authorization Dial-In User Service (RADIUS) servers provide additional security for networks. The RADIUS server maintains a user database, which contains per-user authentication information. RADIUS servers provide a centralized authentication method for:

- Telnet Access
- Web Access
- Console to Switch Access

The **RADIUS Settings** page contains both user-defined and the default RADIUS settings.

To open the **RADIUS Settings** page, click **System Management→Security→RADIUS** in the tree view.

Figure 6-51. RADIUS Settings



The **RADIUS Settings** page contains the following fields:

IP Address — IP address of the authentication port.

Priority (0-65535) — Indicates the port priority. The possible values are 0-65535.

Authentication Port — Identifies the authentication port that is used to verify the RADIUS server authentication.

Number of Retries (1-10) — Number of transmitted requests sent to the RADIUS server before a failure occurs. Possible field values are 1 - 10. Three is the default value. If no host-specific value is specified, the global value applies to each host. Click **Use Default** to use the default value.

Timeout for Reply (1-30) — Amount of the time in seconds the device waits for an answer from the RADIUS server before timing out. Possible field values are 1 - 30. Three is the default value. If no host-specific value is specified, the global value applies to each host. Click **Use Default** to use the default value.

Dead Time (0-2000) — Amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000. If no host-specific value is specified, the global value applies to each host. Click **Use Default** to use the default value.

Key String (0-128 Characters)— Key string used for authenticating and encrypting all RADIUS communications between the device and the RADIUS server. This key must match the RADIUS encryption. If no host-specific value is specified, the global value applies to each host.

Source IP Address — IP Address of device accessing the RADIUS server.

NOTE: Default parameters in this page are user defined.

Default Retries (1-10) — Default number of transmitted requests sent to RADIUS server before a failure occurs.

Default Timeout for Reply (1-30) — The default number of transmitted requests sent to RADIUS server before a failure occurs. Possible field values are 1 - 30.

Default Dead Time (0-2000) — Specifies the default amount of time (in minutes) that a RADIUS server is bypassed for service requests. The range is 0-2000.

Default Key String (0-128 characters) — Default key string used for authenticating and encrypting all RADIUS-communications between the device and the RADIUS server. This key must match the RADIUS encryption.

Source IP Address—Default IP Address of a device accessing the RADIUS server.

Adding a RADIUS Server

1. Open the **RADIUS Settings** page.
2. Click **Add** to display the **Add RADIUS Server** page.
3. Define the fields in the dialog.
4. Click **Apply Changes**.

   The new RADIUS server is added, and the device is updated.

Defining RADIUS Parameters

1. Open the **RADIUS Settings** page.
2. Define the fields in the dialog.
3. Click **Apply Changes**.

   The RADIUS settings are updated to the device.

Modifying the RADIUS Server settings

1. Open the **RADIUS Settings** page.
2. Click **Show All** to display the **RADIUS Servers List**.
3. Modify the fields in the dialog.
4. Click **Apply Changes**.

   The RADIUS Server settings are modified, and the device is updated.

Deleting a RADIUS Server for the RADIUS Servers List

1. Open the **RADIUS Settings** page.
2. Click **Show All** to display the **RADIUS Servers List**.
3. Select a RADIUS Server and check the **Remove** check box.

   The RADIUS server is removed from the list.

Defining RADIUS Servers Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed on the **RADIUS Settings** page.

Table 6-38. RADIUS Server CLI Commands

CLI Command	Description
`radius-server timeout` *timeout*	Sets the interval for which a router waits for a server host to reply.
`radius-server retransmit` *retries*	Specifies the number of times the software searches the list of RADIUS server hosts.
`radius-server deadtime` *deadtime*	Configures unavailable servers to be skipped.
`radius-server key` *key-string*	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS environment.
`radius-server host` *ip-address* `[auth-port` *auth-port-number*`]` `[timeout timeout]` `[retransmit` *retries*`]` `[deadtime` *deadtime*`]` `[key` *key-string*`]` `[source` *source*`]` `[priority` *priority*`]`	Specifies a RADIUS server host.
`show radius-servers`	Displays the RADIUS server settings.

The following is an example of CLI commands:

```
Console (config)# radius-server timeout 5

Console (config)# radius-server retransmit 5

Console (config)# radius-server deadtime 10

Console (config)# radius-server key dell-server

Console (config)# radius-server host 196.210.100.1 auth-port 127
timeout 20

Console# show radius-servers

IP address  Auth   Acct  TimeOut   Retransmit   Deadtime   Source IP  Priority

--------   ----  ----  ------   ---------  -------   -------   ------

172.16.1.1   164    51646  3        3            0                    01
172.16.1.2   164    51646  3        3            0                    02
```

Defining SNMP Parameters

Simple Network Management Protocol (SNMP) provides a method for managing network devices. The device supports SNMP version 1, SNMP version 2 and SNMP version 3.

NOTE: By default, SNMPv2 is automatically enabled on the device. To enable SNMPv3, a local engine ID must be defined for the device. The local engine ID may be a string specified by the user or a generated default string based on the MAC address of the device. For information on how to configure the local engine ID, see **Defining SNMP Global Parameters**.

SNMP v1 and v2

The SNMP agent maintains a list of variables, which are used to manage the device. The variables are defined in the Management Information Base (MIB). The MIB presents the variables controlled by the agent. The SNMP agent defines the MIB specification format, as well as the format used to access the information over the network. Access rights to the SNMP agent are controlled by access strings.

SNMP v3

SNMP v3 also applies access control and a new traps mechanism to SNMPv1 and SNMPv2 PDUs. In addition, the User Security Model (USM) is defined for SNMPv3 and includes:

- **Authentication** — Provides data integrity and data origin authentication.
- **Privacy** — Protects against disclosure of message content. Cipher-Bock-Chaining (CBC) is used for encryption. Either authentication is enabled on a SNMP message, or both authentication and privacy are enabled on a SNMP message. However privacy cannot be enabled without authentication.

- **Timeliness** — Protects against message delay or message redundancy. The SNMP agent compares incoming message to the message time information.
- **Key Management** — Defines key generation, key updates, and key use.

The device supports SNMP notification filters based on Object IDs (OID). OIDs are used by the system to manage device features. SNMP v3 supports the following features:

- Security
- Feature Access Control
- Traps

Authentication or Privacy Keys are modified in the SNMPv3 User Security Model (USM).

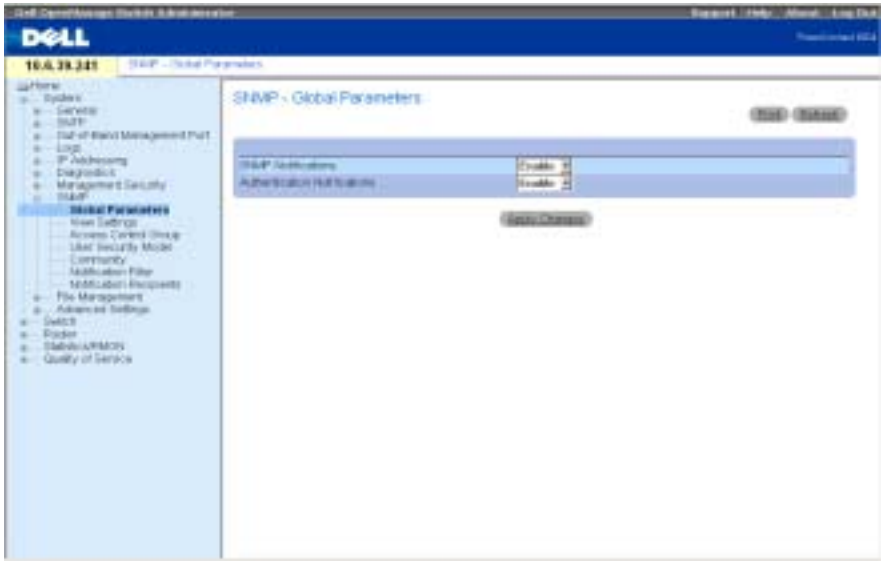
Use the **SNMP** page to define SNMP parameters. To open the **SNMP** page, click **System→SNMP** in the tree view.

Defining SNMP Global Parameters

Use the **Global Parameters** page to enable SNMP and Authentication notifications.

To open the **Global Parameters** page, click **System →SNMP →Global Parameters** in the tree view.

Figure 6-52. Global Parameters



The **Global Parameters** page contains the following parameters:

SNMP Notifications — Enables or disables the device sending SNMP notifications.

Authentication Notifications — Enables or disables the device sending SNMP traps when authentication fails.

Enabling SNMP Notifications

1. Open the **Global Parameters** page.
2. Select **Enable** in the **SNMP Notifications** field.
3. Click **Apply Changes**.

   SNMP notifications are enabled, and the device is updated.

Enabling Authentication Notifications

1. Open the **Global Parameters** page.
2. Select **Enable** in the **Authentication Notifications** field.
3. Click **Apply Changes**.

   Authentication notifications are enabled, and the device is updated.

Enabling SNMP Notifications Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **Global Parameters** page.

Table 6-39. SNMP Notification CLI Commands

CLI Command	Description
`snmp-server engineID local {`*`engineid-string`*` | default}`	Specifies the SNMP engine ID on the local device.
`snmp-server enable traps`	Enables the device to send Simple Network Management Protocol traps.
`snmp-server trap authentication`	Enables the device to send Simple Network Management Protocol traps when authentication fails.
`show snmp`	Shows the current SNMP device configuration.

The following is an example of CLI commands:

```
Console (config)# snmp-server enable traps
Console (config)# snmp-server trap authentication
Console (config)# end
Console# show snmp

Community-String  Community-Access     IP address
------------      -----------------    -----------------
public            read only            All
private           read write           172.16.1.1
private           read write           172.17.1.1

OOB management stations
Community-String  Community-Access     IP address
------------      -----------------    -----------------
private           read write           176.16.8.9

Traps are enabled.
Authentication trap is enabled.

Trap-Rec-Address  Trap-Rec-Community   Version
192.122.173.42     public              2

OOB trap receivers
Trap-Rec-Address  Trap-Rec-Community   Version
176.16.8.9         public              2

System Contact: Robert
System Location: Marketing
```

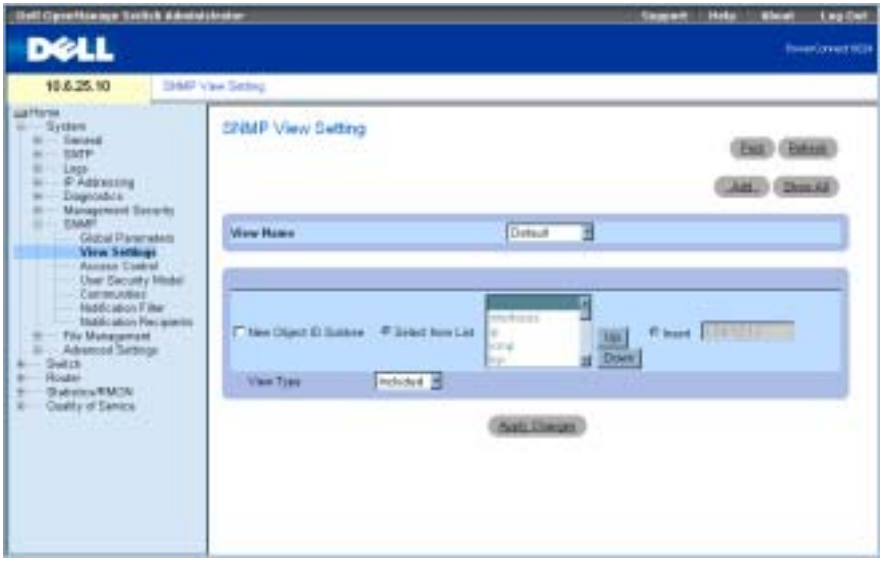
Defining SNMP Views

SNMP views provide or block access to device features or feature aspects. For example, a view can be defined which states that SNMP group A has read-only access to routing, while SNMP group B has read-write access to routing. Feature access is granted via the MIB name or MIB Object ID.

Use the **SNMP View Setting** page to define SNMP views.

To open the **SNMP View Setting** page, click **System →SNMP →View Settings** in the tree view.

Figure 6-53. SNMP View Setting



The **SNMP View Setting** page contains the following fields:

View Name — Contains a list of user-defined views. A view name can contain a maximum of 30 alphanumeric characters.

New Object ID Subtree — Specifies the device feature OID included or excluded in the SNMP view.

View Type — When checked, enables access to a selected feature or feature aspect in the SNMP view.

Adding a View

1. Open the **SNMP View Setting** page.
2. Click **Add**.

   The **Add A View** page opens:

Figure 6-54. Add A View

3 Define the relevant fields.

4 Click **Apply Changes**.

The SNMP view is added, and the device is updated.

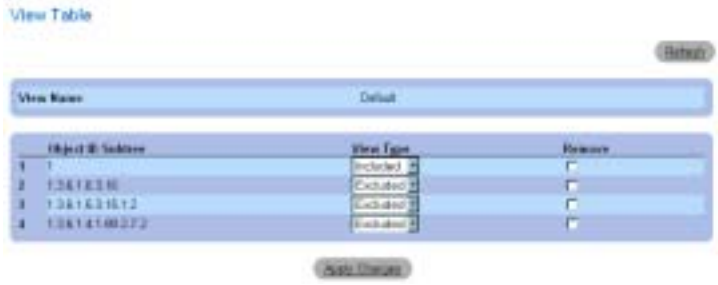
Displaying the View Table

1 Open the **SNMP View Setting** page.

2 Click **Show All**.

The **View Table** page opens:

Figure 6-55. View Table



Removing SNMP Views

1 Open the **SNMP View Setting** page.

2 Click **Show All**.

The **View Table** page opens.

3 Select a SNMP view.

4 Check the **Remove** check box.

5 Click **Apply Changes**.

The SNMP view is deleted, and the device is updated.

Defining SNMP Views Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **SNMP View Setting** page.

Table 6-40. SNMP View CLI Commands

CLI Command	Description
`snmp-server view` *`view-name oid-tree`* `{included | excluded}`	Creates or updates a view entry.
`show snmp views` [*`viewname`*]	Displays the configuration of views.

The following is an example of CLI commands:

```
Console (config)# snmp-server view user1 1 included
Console (config)# end
Console # show snmp views

Name              OID Tree              Type
-------------     -----------------     --------
user1             iso                   included
Default           iso                   included
Default           snmpVacmMIB           excluded
Default           usmUser               excluded
Default           rndCommunityTable     excluded
DefaultSuper      iso                   included
```

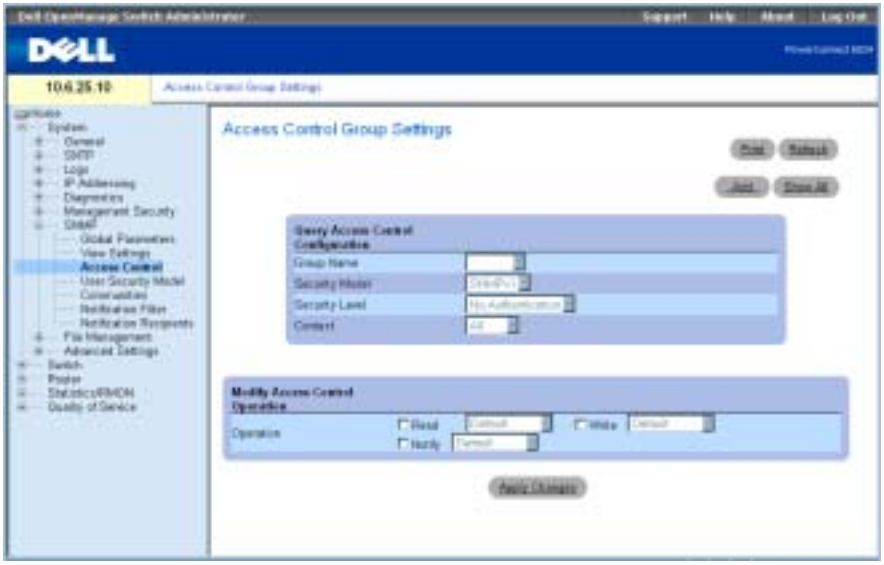
Defining SNMP Access Control

The **Access Control Group** page provides information for creating SNMP groups, and assigning SNMP access privileges. Groups allow network managers to assign access rights to specific device features or features aspects.

The Out-of-Band port is treated as a separate device when using SNMP features. Views can be limited to Out-of-Band MIBs, device MIBs or to all MIBs.

To open the **Access Control Group** page, click **System →SNMP →Access Control** in the tree view.

Figure 6-56. Access Control Group



The **Access Control Group** page contains the following fields:

Group Name — Contains a list of user-defined groups to which access control rules are applied. A group name can contain a maximum of 30 alphanumeric characters.

Security Model — Defines the SNMP version attached to the group. The possible field values are:

SNMPv1 — SNMPv1 is defined for the group.

SNMPv2 — SNMPv2 is defined for the group.

SNMPv3 — SNMPv3 is defined for the group.

Security Level — The security level attached to the group. Security levels apply to SNMPv3 groups only. The possible field values are:

No Authentication — Neither Authentication nor Privacy security levels are assigned to the group.

Authentication — Authenticates SNMP messages without encrypting them.

Privacy — Authenticates SNMP messages and encrypts them.

Operation — Defines group access rights. The possible field values are:

Read — Select a view that restricts management access to viewing the contents of the agent. If no view is selected, all objects except the community-table, SNMPv3 user and access tables can be viewed.

Write — Select a view that permits management read-write access to the contents of the agent but not to the community.

Notify — Select a view that permits sending SNMP traps or informs.

Context — Context for which the access group is configured. The possible field values are:

Router — Access group is configured for inband management.

OOB — Access group is configured for Out-of-band management.

All — Access group is configured for both inband and Out-of-band management

Defining SNMP Groups

1. Open the **Access Control Group** page.
2. Click **Add**.

   The **Add an Access Control Group** page opens:

Figure 6-57. Add an Access Control Group

3. Define the fields.
4. Click **Apply Changes**.

   The group is added, and the device is updated.

Displaying the Access Table

1. Open the **Access Control Group** page.
2. Click **Show All**.

   The **Access Table** page opens:

Figure 6-58. Access Table

Deleting a Group

1. Open the **Access Control Group** page.
2. Click **Show All**.

   The **Access Table** opens.
3. Select a group.
4. Check the **Remove** checkbox.
5. Click **Apply Changes**.

   The group is deleted, and the device is updated.

Defining SNMP Access Control Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **Access Control Group** page.

Table 6-41. SNMP Access Control CLI Commands

CLI Command	Description
`snmp-server group` *groupname* `{v1 | v2 | v3 {noauth | auth | priv}} [read` *readview*`] [write` *writeview*`] [notify` *notifyview* `]`	Configure a new Simple Network Management Protocol (SNMP) group, or a table that maps SNMP users to SNMP views.
`show snmp groups [`*groupname*`]`	Displays the configuration of groups

The following is an example of the CLI commands:

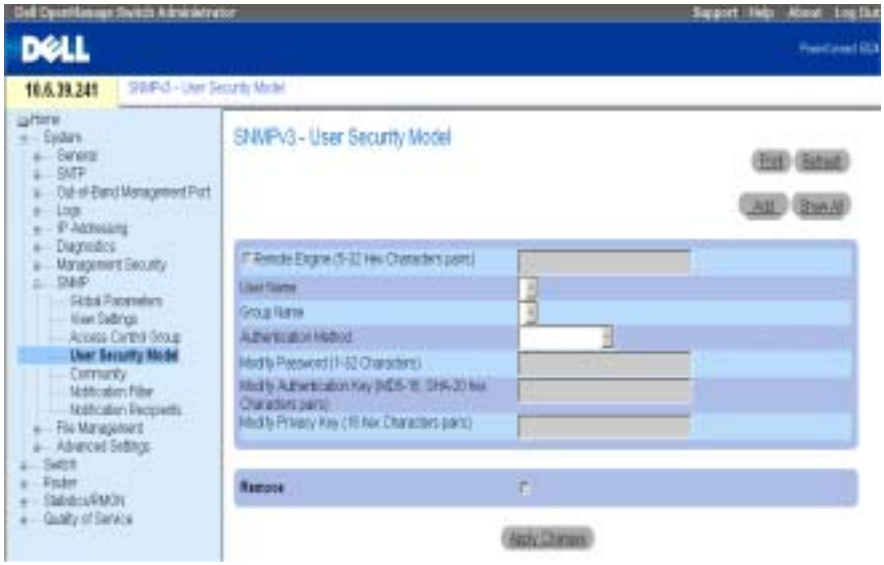
```
Console (config)# snmp-server group user-group v3 priv read user-
view
```

Assigning SNMP User Security

The **SNMPv3 User Security Model (USM)** page enables assigning system users to SNMP groups, as well as, defining the user authentication method.

To open the **SNMPv3 User Security Model (USM)** page, click **System→SNMP →User Security Model** in the tree view.

Figure 6-59. SNMPv3 User Security Model (USM)



The **SNMPv3 User Security Model (USM)** page contains the following fields:

Engine ID — Identifies the remote SNMPv3 enabled device to which the selected user is connected.

Remote Engine ID — Indicates that the user is configured on a remote SNMPv3 enabled device. If the engine ID is defined, remote devices receive inform messages.

User Name — Contains a list of user-defined user names.

Group Name — Contains a list of user-defined SNMP groups. SNMP groups are defined in the **Access Control Group** page.

Authentication Method — Specifies the authentication method used to authenticate users. The possible field values are:

None — No user authentication is used.

MD5 Password — Users are authenticated using the HMAC-MD5-96 authentication level. The user should specify a password.

SHA Password — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter a password.

MD5 Key — Users are authenticated using the HMAC-MD5-96 authentication level. The user should enter authentication and privacy keys.

SHA Key — Users are authenticated using the HMAC-SHA-96 authentication level. The user should enter authentication and privacy keys.

Password (0-32 Characters) — Modifies the user defined password for the group. Passwords can contain a maximum of 32 characters. Passwords are defined only if the authentication method is MD5 or SHA Password.

Authentication Key(MD5-16; SHA-20 hexa chars) — Specify the authentication key. An authentication key is defined only if the authentication method is MD5 Key or SHA Key.

Privacy Key (16 hexa chars) — Specify a password for authenticating and generating a DES key for privacy. A privacy key is defined only if the authentication method is MD5 Key or SHA Key.

Remove — When checked, removes the specified user from the specified group.

Adding SNMPv3 Users to a Group

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Add**.

   The **Add SNMPv3 User Name** page opens:

Figure 6-60. Add SNMPv3 User Name

3. Define the relevant fields.
4. Click **Apply Changes**.
5. The user is added to the group, and the device is updated.

Viewing the User Security Model Table

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Show All**.

   The **SNMPv3 User Security Model Table** opens:

Figure 6-61. SNMPv3 User Security Model Table

Deleting a User Security Model Table Entry

1. Open the **SNMPv3 User Security Model (USM)** page.
2. Click **Show All**.

   The **SNMPv3 User Security Model Table** page opens.
3. Select an entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The entry is deleted, and the device is updated.

Defining SNMP Users Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **SNMPv3 User Security Model (USM)** page.

Table 6-42. SNMP User CLI Commands

CLI Command	Description
`snmp-server user` *username groupname* `[remote` *engineid-string*`][auth-md5` *password* `| auth-sha` *password* `| auth-md5-key` *md5-des-key* `| auth-sha-key` *sha-des-key*`]`	Configures a new SNMP V3 user.
`show snmp users [`*username*`]`	Displays the configuration of users.

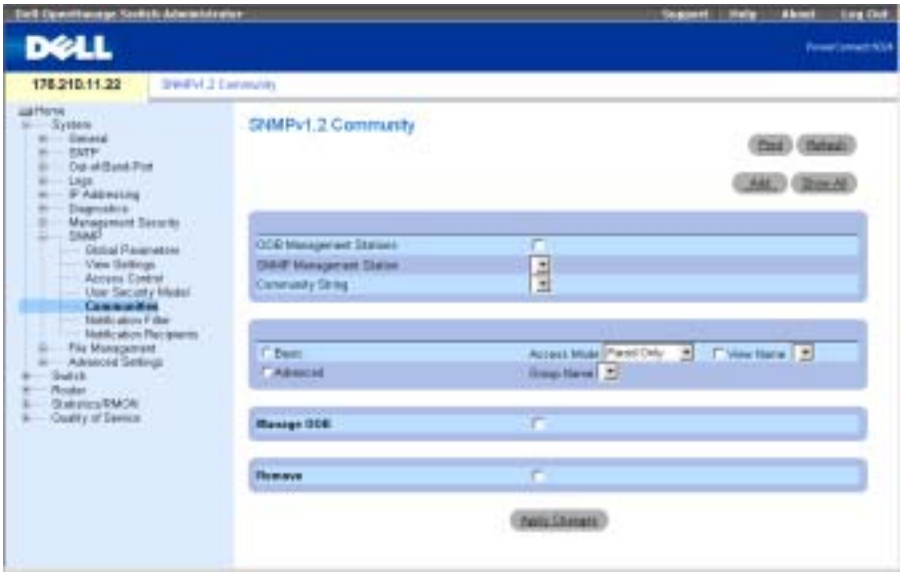
```
Console (config)# snmp-server user John auth-md5 1234
Console (config)# end
Console (config)# show snmp users

Name          Group Name     Auth Method      Remote
-------       ----------     -----------      ------
John          user-group     md5
```

Defining Communities

Access rights are managed by defining communities on the **SNMPv1, 2 Community** page. When the community names are changed, access rights are also changed. SNMP Comminutes are defined only for SNMP v1 and SNMP v2.

To open the **SNMPv1, 2 Community** page, click **System→SNMP→Communities** in the tree view.

Figure 6-62. SNMPv1, 2 Community



The **SNMPv1, 2 Community** page contains the following fields:

OOB Management Station — Select this checkbox to create a separate SNMP community for the Out-of-Band port. If this checkbox is not selected, the device is accessed by the management station via the inband ports.

SNMP Management Station — Contains a list of management station IP address. for which community strings have been defined.

NOTE: Only superusers can use the same community to configure Out-of-Band and inband ports.

Community String — Contains a list of user-defined community strings that act as a password and are used to authenticate the SNMP management station to the device. A community string can contain a maximum of 20 characters.

Basic — Enables SNMP Basic mode for the selected community. The possible field values are:

Access Mode — Defines the access rights of the community. The possible field values are:

Read-Only — Management access is restricted to read-only, and changes cannot be made to the community.

Read-Write — Management access is read-write and changes can be made to the device configuration, but not to the community.

SNMP-Admin — User has access to all device configuration options as well as rights to modifying the community.

View Name — Contains a list of user-defined SNMP views

Advanced — Contains a list of user-defined groups. When SNMP Advanced mode is selected, the SNMP access control rules comprising the group are enabled for the selected community. The Advanced mode also enables SNMP groups for specific SNMP communities. The SNMP Advanced mode is defined only with SNMPv3.

Manage OOB — If this checkbox is selected , SNMP management is provided to Out-of-Band management stations connected to the device via the Out-of-Band port only.

Remove — When checked, removes a community.

Defining a New Community

1. Open the **SNMPv1, 2 Community** page.
2. Click **Add**.

   The **Add SNMPv1,2 Community** page opens:

Figure 6-63. Add SNMPv1,2 Community

3. Complete the relevant fields.

   In addition to the fields in the **SNMPv1, 2 Community** page, the **Add SNMPv1,2 Community** page contains the **All (0.0.0.0)** field, which indicates if an SNMP community is defined for a specific management station or for all management stations.
4. Click **Apply Changes**.

   The new community is saved, and the device is updated.

Deleting Communities

1. Open the **SNMPv1, 2 Community** page.
2. Click **Show All**.

   The **SNMPv1,2 Community Tables** page opens.
3. Select a community and check the **Remove** check box.
4. Click **Apply Changes**.

   The community entry is deleted, and the device is updated.

Configuring Communities Using CLI Commands

The following table summarizes equivalent CLI commands for defining fields displayed in the **SNMPv1, 2 Community** page.

Table 6-43. SNMP Community CLI Commands

CLI Command	Description
`snmp-server community` *`community`* `[ro | rw | su] [`*`ip-address`*`][view` *`view-name`*`][type {router | oob}]`	Sets up the community access string to permit access to the SNMP protocol.
`snmp-server community-group` *`community group-name`* `[`*`ip-address`*`] [type {router | oob}]`	Sets up comunity access string to permit limited access to the SNMP protocol based on group access rights.
`show snmp`	Displays the current SNMP device configuration.

The following is an example of CLI commands:

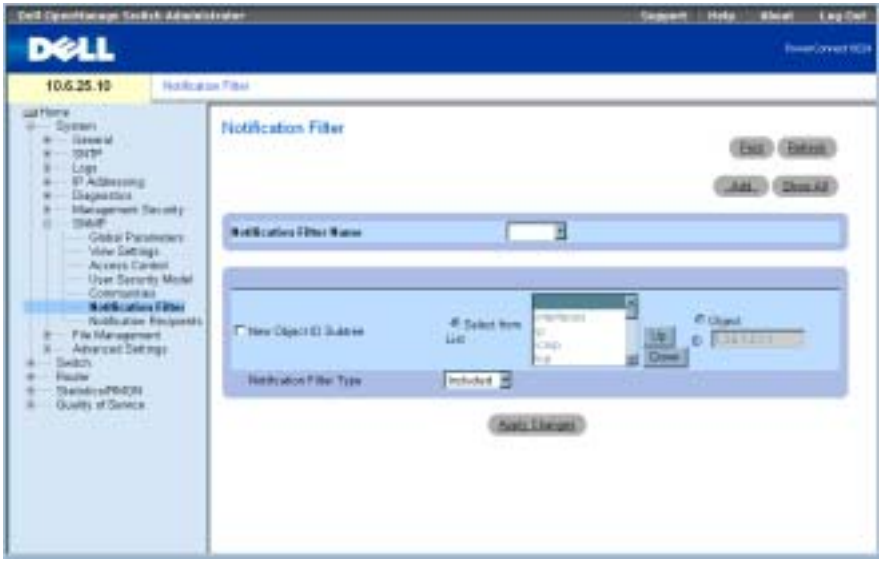
```
Console (config)# snmp-server community dell ro 10.1.1.1
```

Defining SNMP Notification Filters

The **Notification Filter** page permits filtering traps based on OIDs. Each OID is linked to a device feature or a feature aspect. The **Notification Filter** page also allows network managers to filter notifications.

To open the **Notification Filter** page, click **System→SNMP →Notification Filters** in the tree view.

Figure 6-64. Notification Filter



The **Notification Filter** page contains the following fields:

Notification Filter Name — Contains a list of user-defined notification filters. A notification filter name can contain a maximum of 30 characters.

New Object Identifier Subtree — The OID for which notifications are sent or blocked. If a filter is attached to an OID, traps or informs are generated and sent to the trap recipients. Object IDs are either selected from the *Select from List* box or specified in the *Object ID* field.

Notification Filter Type — Indicates whether informs or traps are sent regarding the OID to the trap recipients.

Excluded — Restricts sending OID traps or informs.

Included — Sends OID traps or informs.

Adding SNMP Filters

1. Open the **Notification Filter** page.
2. Click **Add**.

   The **Add Filter** page opens:

Figure 6-65. Add Filter

3 Define the relevant fields.

4 Click **Apply Changes**.

The new filter is added, and the device is updated.

Displaying the Filter Table

1 Open the **Notification Filter** page.

2 Click **Show All**.

The **Filter Table** page opens:

Figure 6-66. Filter Table

Removing a Filter

1 Open the **Notification Filter** page.

2 Click **Show All**.

The **Filter Table** page opens.

3 Select a **Filter Table** entry.

4 Check the **Remove** the check box.

The filter entry is deleted, and the device is updated.

Configuring Notification Filters Using CLI Commands

The following table summarizes equivalent CLI commands for defining fields displayed in the **Notification Filter** page.

Table 6-44. SNMP Notification Filter CLI Commands

CLI Command	Description
`snmp-server filter` *`filter-name oid-tree`* `{included | excluded}`	Creates or updates an SNMP notification filter.
`show snmp filters` [*`filtername`*]	Displays the configuration of SNMP notification filters

The following is an example of CLI commands:

```
Console (config)# snmp-server filter user1 1 included
Console(config)# end
Console # show snmp filters

Name            OID Tree          Type
-----------     -------------     --------
user1           iso               Included
```

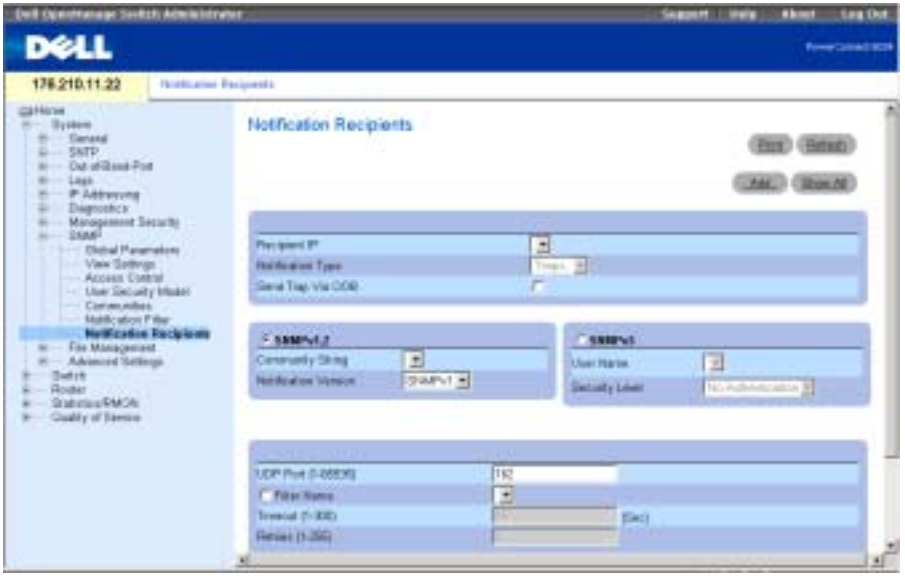
Defining SNMP Notification Recipients

The **Notification Recipients** page contains information for defining filters that determine whether traps are sent to specific users, and the trap type sent. SNMP notification filters provide the following services:

- Identifying Management Trap Targets
- Trap Filtering
- Selecting Trap Generation Parameters
- Providing Access Control Checks

To open the **Notification Recipients** page, click **System→SNMP→Notification Recipient** in the tree view.

Figure 6-67. Notification Recipients



The **Notification Recipients** page contains the following fields:

Recipient IP — Contains a user-defined list of notification recipients IP addresses.

Notification Type — The type of notification sent. The possible field values are:

Trap — Traps are sent.

Inform — Informs are sent.

SNMPv1,2 — SNMP versions 1 or 2 are enabled for the selected recipient. The possible field values are:

Community String — Contains a list of community strings. Select one to be sent with the notification.

Notification Version — Determines the notification version. The possible field values are:

SNMP V1 — SNMP version 1 traps are sent.

SNMP V2 — SNMP version 2 traps or informs are sent.

SNMPv3 — SNMP version 3 is enabled for the selected recipient. The possible field values are:

User Name — Contains a list of users. Select one to generate notifications.

Security Level — The security level attached to notifications. The possible field values are:

No Authentication — The packet is neither authenticated nor encrypted.

Authentication — The packet is authenticated.

Privacy — The packet is both authenticated and encrypted.

UDP Port (1-65535) — UDP port used to send notifications. The default is 162.

Filter Name — Check this check box to apply a user-defined SNMP filter to notifications and select an SNMP filter from the list.

Timeout (1-300) — Amount of time (seconds) the device waits before resending informs. The default is 15 seconds.

Retries (1-255) — Maximum number of times the device resends an inform request. The default is 3.

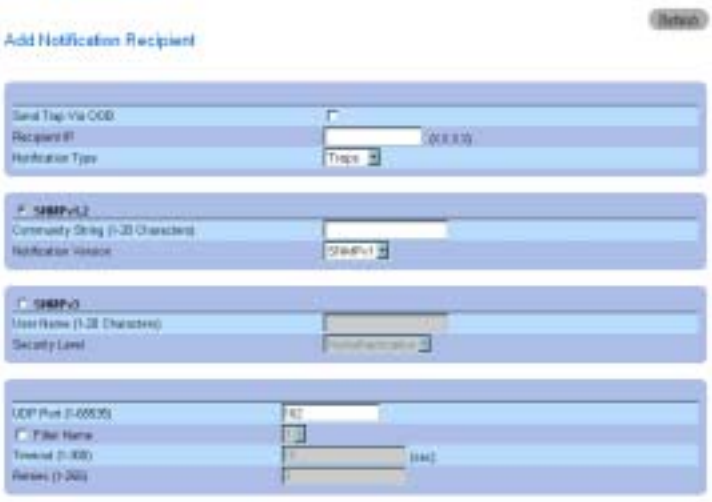
Remove Notification Recipient — When checked, removes the selected notification recipient.

Adding a New Notification Recipient

1. Open the **Notification Recipients** page.
2. Click **Add.**

   The **Add Notification Recipient** page opens:

Figure 6-68. Add Notification Recipient



3 Define the relevant fields.

4 Click **Apply Changes**.

The notification recipient is added, and the device is updated.

Displaying the Notification Recipients Tables

1 Open **Notification Recipients** page.

2 Click **Show All**.

The **Notification Recipients Table** page open:

Figure 6-69. Notification Recipients Table

Deleting Notification Recipients

1. Open the **Notification Recipients** page.
2. Click **Show All**.

   The **Notification Recipients Tables** page open.
3. Select one or more notification recipients in the **SNMPV1,2 Notification Recipient** and/or **SNMPv3 Notification Recipient Tables**.
4. Click **Apply Changes**.

   The recipients are deleted, and the device is updated.

Defining SNMP Notification Recipients Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **Notification Recipients** page.

Table 6-45. SNMP Notification Recipients CLI Commands

CLI Command	Description
`snmp-server host {`*`ip-address	hostname`*`} community-string [traps	informs] [1	2] [udp-port port] [filter filtername] [timeout seconds] [retries retries]`	Creates or updates a notification recipient receiving notifications in SNMP version 1 or 2.
`snmp-server v3-host {`*`ip-address	hostname`*`} username [traps	informs] {noauth	auth	priv} [udp-port port] [filter filtername] [timeout seconds] [retries retries]`	Creates or updates a notification recipient receiving notifications in SNMP version 3.
show snmp	Displays the current SNMP device configuration.

The following is an example of CLI commands:

```
Console (config)# snmp-server host 12.1.1.1 Dell-community
Console (config)# end
Console# show snmp
Community-String  Community-Access  View name  IP address     Type
----------------  ----------------  -----      ----------     ----
Community-String  Group name        IP address        Type
----------------  ----------        ----------        ----

OOB management stations
Community-String  Community-Access  View name  IP address     Type
----------------  ----------------  ---------  ----------     ----
Community-String  Group name        IP address        Type
----------------  ----------        ----------        ----

Traps are enabled.
Authentication-failure trap is enabled.


Version 1,2 notifications
Target    Type   Community  Version   Udp     Filter    To     Retries
Address                               Port    name      Sec
--------  ----   ---------  -------   -----   -------   ---    -------
12.1.1.1  Trap   Dell_comm  2         162               1500   3
                 unity

OOB Notification Receivers
Target    Type   Community  Version   Udp     Filter    To     Retries
Address                               Port    name      Sec
--------  ----   ---------  ----      ----    -------   ---    -------
```

```
Version 3 notifications
Target    Type   Username   Security  Udp    Filter    To    Retries
Address                     Level     Port   name      Sec
--------  ----   --------   -------   ----   -------   ---   -------

OOB Notification Receivers
Target    Type   Username   Security  Udp    Filter    To    Retries
Address                     Level     Port   name      Sec
--------  ----   --------   -------   ----   -------   ---   -------
```

Managing Files

Use the **File Management** page to manage device software, the image file, and the configuration files. Files can be downloaded or uploaded via a TFTP server.

Management File Overview

The management file structure consists of the following files:

- **Startup configuration file** — Retains the exact device configuration when the device is powered down or rebooted. The startup file maintains configuration commands, and configuration commands from the running configuration file can be saved to the startup file.
- **Running configuration file**—Contains all startup file commands, as well as all commands entered during the current session. After the device is powered down or rebooted, all commands stored in the running configuration file are lost. During the startup process all commands in the startup file are copied to the running configuration file and applied to the device. During the session, all new commands entered are added to the commands existing in the running configuration file. Commands are not overwritten. To update the startup file, before powering down the device the running configuration file must be copied to the startup configuration file. The next time the device is restarted, the commands are copied back into the running configuration file from the startup configuration file
- **Backup Configuration File** — Contains a backup copy of the device configuration. The backup file changes when the running configuration file or the startup file is copied to the backup file. The commands copied into the file replace the existing commands saved in the backup file. The backup file contents can be copied to either the running configuration or the startup configuration files.
- **Image Files**—System images are saved in two Flash sectors called images (Image 1 and Image 2). The active image stores the active copy; while the other image stores a second copy. The device boots and runs from the active image. If the active image is corrupt, the system automatically boots from the non-active image. This is a safety feature for faults occurring during the boot upgrade process.

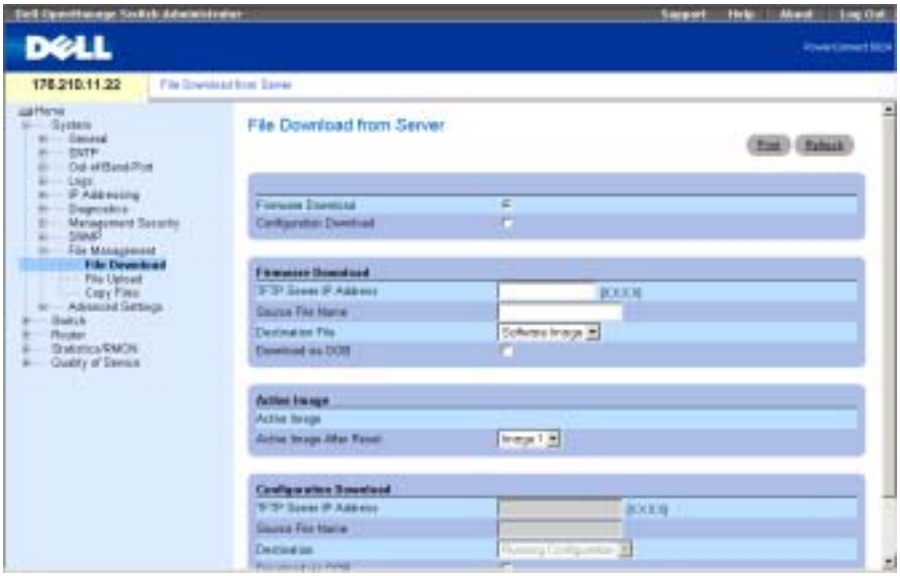
To open the **File Management** page, click **System→File Management** in the tree view.

Downloading Files

The **File Download From Server** page contains fields for downloading the software from the TFTP server to the device. The image file can also be downloaded from the **File Download from Server** page.

To open the **File Download From Server** page, click **System→File Management→File Download** in the tree view.

Figure 6-70. File Download From Server



The **File Download From Server** page contains the following fields:

Firmware Download — When selected, indicates that the firmware file is downloaded. If this option is selected, the **Configuration Download** fields are grayed out.

Configuration Download — When selected, indicates that the configuration file is downloaded. If **Configuration Download** is selected, the **Firmware Download** fields are grayed out.

Firmware TFTP Server IP Address — TFTP server IP address from which files are downloaded.

Firmware Source File Name — Firmware file to be downloaded.

Firmware Destination File — Determines whether the file is downloaded to the image file or boot file.

Firmware Download via OOB—Downloads the Firmware file via the out-of-band management port.

Active Image — Image file that is currently active.

Active Image After Reset — The image file that is active after the device is reset. Possible values are as follows:

Image 1 — The Image 1 file is active after device is reset.

Image 2 — The Image 2 file is active after device is reset.

Configuration File TFTP Server IP Address — TFTP Server IP Address via which the configuration files are downloaded.

Configuration File Source File Name — Configuration file to be downloaded.

Configuration File Destination — The destination file to which to the configuration files is downloaded. Possible values are:

Running Configuration — Downloads the running configuration files.

Startup Configuration — Downloads the startup config files.

Backup Configuration — Downloads the backup config files.

Configuration Download via OOB—Downloads the Configuration file via the out-of-band management port.

Downloading Files

1. Open the **File Download From Server** page.
2. Verify the IP address of the TFTP server and ensure that the software image or boot file to be downloaded is available on the TFTP server.
3. Complete the **TFTP Server IP Address**, **Source File Name** (full path without TFTP server IP address), and the **Destination File** (software image or boot) fields.

NOTE: The image file image overwrites the non-active image. It is recommended to designate that the non-active image will become the active image after reset, and then to reset the device following the download.

4. Click **Apply Changes**.

   The software is downloaded to the device.

Activating Image Files

1. Open the **File Download From Server** page.
2. Select the image to activate from the **Active Image After Reset** drop-down menu.
3. Click **Apply Changes**.

   The image file is selected.

NOTE: To activate the selected Image file, reset the device. For information about resetting the device, see "Resetting the Device."

Downloading Files Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **File Download From Server** page.

Table 6-46. Download CLI Commands

CLI Command	Description
`copy` *source-url destination-url*	Copies any file from a source to a destination.

The following is an example of the CLI commands:

```
Console # copy tftp://172.16.101.101/file1 image


Accessing file 'file1' on 172.16.101.101...

Loading file1 from 172.16.101.101:

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

[OK]

Copy took 0:01:11 [hh:mm:ss]
```

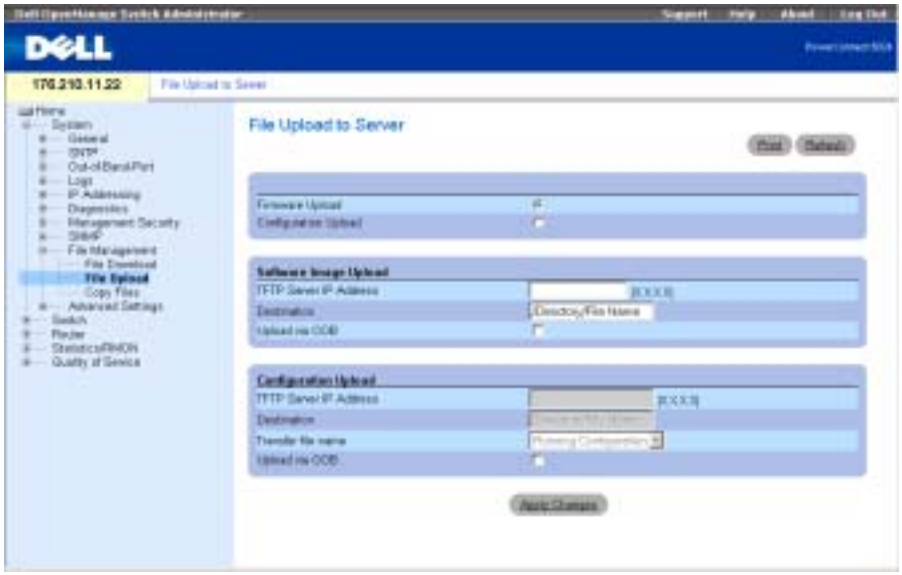
NOTE: Each "!" indicates that the file download is progressing successfully.

Uploading Files

The **File Upload to Server** page contains fields for uploading the files from the TFTP server to the device. The Image file can also be uploaded from the **File Upload to Server** page.

To open the **File Upload to Server** page, click **System→File Management→File Upload** in the tree view.

Figure 6-71. File Upload to Server



The **File Upload to Server** page contains the following fields:

Firmware Upload — Indicates that the firmware file is uploaded. If **Firmware Upload** is selected, the **Configuration Upload** fields are grayed out.

Configuration Upload — Indicates that the configuration file is uploaded. If **Configuration Upload** is selected, the **Firmware Upload** fields are grayed out.

Software Image Upload TFTP Server IP Address — TFTP server IP address to which the software image is uploaded.

Software Image Upload Destination — The Software Image file path to which the file is uploaded.

Software Image Upload via OOB—Indicates that the software image is uploaded via the out-of-band management port.

Configuration Upload TFTP Server IP Address — TFTP server IP address to which the configuration file is uploaded.

Configuration Upload Destination — The configuration file path to which the file is uploaded.

Configuration Upload Transfer File Name — The software file that is uploaded. Possible field values are:

Running Configuration — Uploads the running configuration file.

Startup Configuration — Uploads the startup config files.

Backup Configuration — Uploads the backup config files.

Configuration Upload via OOB—Indicates that the Configuration file is uploaded via the out-of-band management port.

Uploading Files

1. Open the **File Upload to Server** page.
2. Define the applicable fields in the page.
3. Click **Apply Changes**.

   The software is uploaded to the server.

Uploading Files Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed on the **File Upload to Server** page.

Table 6-47. Upload CLI Commands

CLI Command	Description
`copy source-url destination-url`	Copies any file from a source to a destination.

The following is an example of the CLI command:

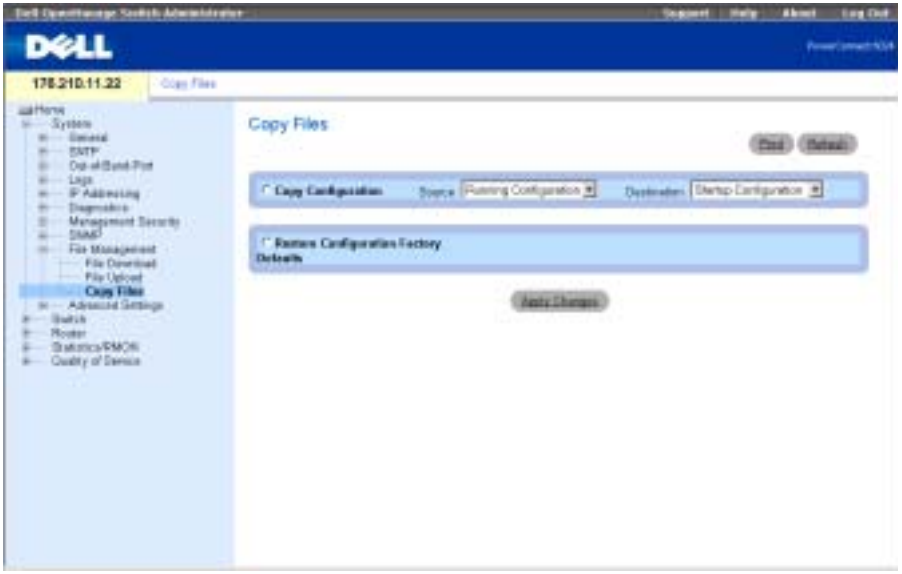
```
-----------------------------------------------------

console#copy image tftp:16.1.1.200/file1
```

Copying Files

Use the **Copy Files** page to copy and restore configuration defaults.

To open the **Copy Files** page, click **System→File Management→Copy** in the tree view.

Figure 6-72. Copy Files



The **Copy Files** page contains the following fields:

Copy Configuration — Specifies that a configuration file should be copied.

Source — The configuration source file (running, startup, backup) from which the file is copied.

Destination — The destination configuration file (running, startup, backup) to which the file is copied.

Restore Configuration Factory Defaults — When checked, specifies that the factory configuration default files should be reset. Unchecked maintains the current configuration settings.

NOTE: Copying files to the running configuration file only adds configuration data; it does not replace the file.

Copying Files

1. Open the **Copy Files** page.
2. Select **Copy** or **Restore**, and complete the fields.
3. Click **Apply Changes**.

   The file is copied.

Copying Files Using CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **Copy Files** page.

Table 6-48. Copy File CLI Commands

CLI Command	Description
`copy source-url destination-url`	Copies any file from a source to a destination.
`delete startup-config`	Deletes the startup configuration file.

The following is an example of the CLI commands:

```
Console# delete startup-config
```

Defining Advanced Settings

Use Advanced Settings to set miscellaneous global attributes of the device. The changes to these attributes are applied only after the device is reset. Click **System→Advanced Settings** in the tree view to open the **Advanced Settings** page.

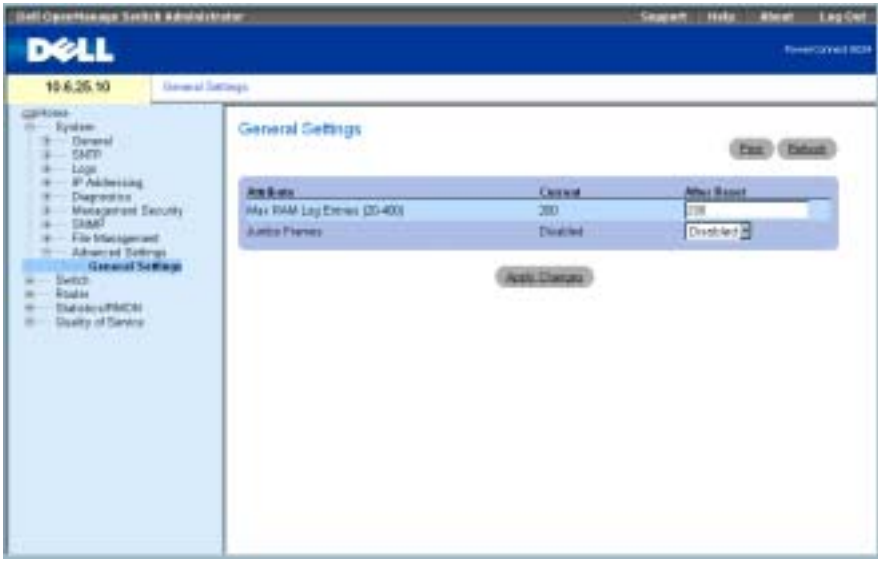
The the **Advanced Settings** page contains a link for configuring general settings.

Configuring General Settings

Use the **General Settings** page to define general device parameters.

To open the **General Settings** page, click **System > Advanced Settings > General** in the tree view.

Figure 6-73. General Settings



The **General Settings** page contains the following fields:

Current — Maximum number of entries.

After Reset— Maximum number of entries after the device is reset. By entering a value in this column, memory is allocated to the field table.

Max RAM Log Entries (20-400) — Maximum number of RAM Log table entries. The default value is 200 entries.

Jumbo Frames — Enables the transportation of identical data in fewer frames. This ensures less overhead, lower processing time, and fewer interrupts. Internal frames may be effected by enabling Jumbo frames.

Enabling Jumbo Packets

1. Open the **General Settings** page.
2. Select **Enabled** in the **Jumbo packets** field.
3. Click **Apply Changes**.

   Jumbo packets are enabled on the device.

Viewing General Settings Using the CLI Commands

The following table summarizes the equivalent CLI commands for defining fields displayed in the **General Settings** page.

Table 6-49. General Settings CLI Commands

CLI Command	Description
`logging buffered size` *`number`*	Sets the number of syslog messages stored in the internal buffer (RAM).
`port jumbo-frame`	Enables jumbo packets for the device.

The following is an example of the CLI commands:

```
Console (config)# logging buffered size 300
Console (config)#port jumbo-frame
```

7

Configuring Switch Information

This section provides all system operations and general information for configuring network security, ports, address tables, GARP, VLANs, Spanning Tree, Port Aggregation, and Multicast Support.

Configuring Network Security

Use the **Network Security** page to set network security through both access control lists and locked ports. To open the **Network Security** page, select **Switch→Network Security**.

The **Network Security** page provides links that enable you to configure port based authentication, port security, IP based ACLs, MAC based ACLs and ACL bindings.

Port Based Authentication (802.1x)

Port based authentication enables authenticating system users on a per port basis via an external server. Only authenticated and approved system users can transmit and receive data. Ports are authenticated via the RADIUS server using the Extensible Authentication Protocol (EAP).

The 802.1x network has three components:

- **Authenticators** — Specifies the port that is authenticated before permitting system access.
- **Supplicants** — Specifies host connected to the authenticated port requesting to access the system services.
- **Authentication Server** — Specifies the external server, for example, the RADIUS server that performs the authentication on behalf of the authenticator, and indicates whether the user is authorized to access system services.

Port based authentication creates two access states:

- **Controlled Access** — Permits communication between the user and the system, if the user is authorized.
- **Uncontrolled Access** — Permits uncontrolled communication regardless of the port state.

The device currently supports Port Based Authentication via RADIUS servers.

Advanced Port Based Authentication

Advanced Port Based Authentication enables multiple hosts to be attached to a single port. Advanced Port Based Authentication requires only one host to be authorized for all hosts to have system access. If the port is unauthorized all attached hosts are denied access to the network.

Advanced Port Based Authentication also enables VLAN based authentication. Specific VLANs in the switch are always available, even if specific ports attached to the VLAN are unauthorized. For example, Voice over IP does not require authentication, while data traffic requires authentication. VLANs for which authorization is not required can be defined. Unauthenticated VLANs are available to users, even if the ports attached to the VLAN are defined as authorized.

Advanced Port Based Authentication is implemented in the following modes:

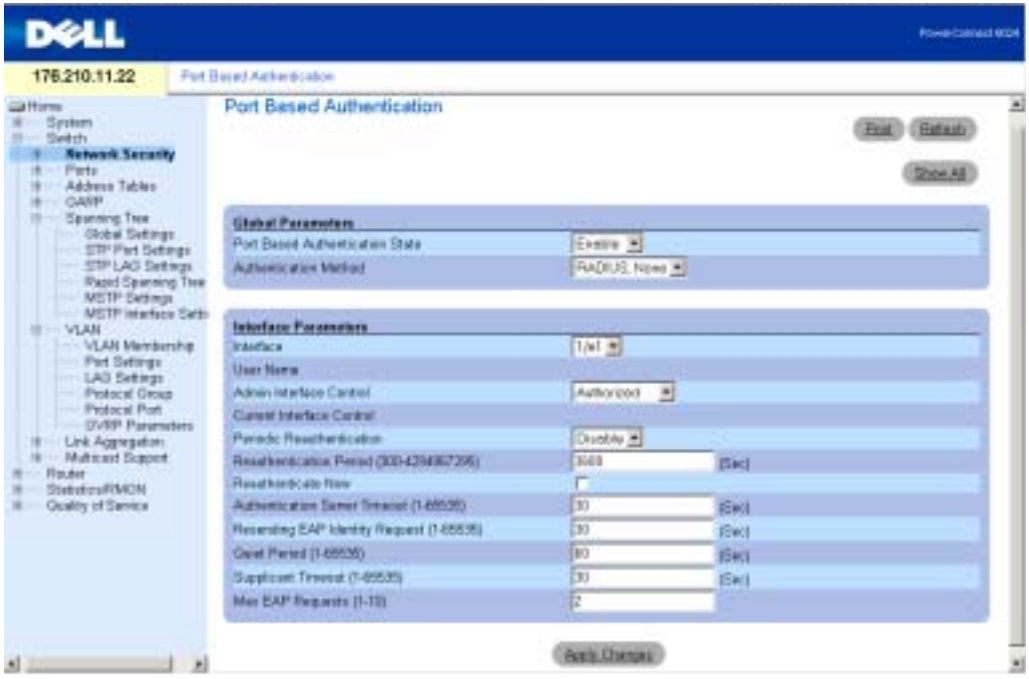
- **Single Host Mode** — Enables only the authorized host to access the port.
- **Multiple Host Mode** — Enables multiple hosts to be attached to a single port. Only one host must be authorized for all hosts to access the network. If the host authentication fails or an EAPOL-logoff message is received, all attached clients are denied network access.

Configuring Port Based Authentication

The **Port Based Authentication** page contains fields for configuring port based authentication.

To open the **Port Based Authentication** page, click **Switch** →**Network Security** →**Port Based Authentication**.

Figure 7-1. Port Based Authentication



The **Port Based Authentication** page contains the following fields:

Port Based Authentication State — Permits port based authentication on the device. The possible field values are:

Enable — Enables port based authentication on the device.

Disable — Disables port based authentication on the device.

Authentication Method — The Authentication method used. The possible field values are:

RADIUS, None — Indicates that port authentication is performed first via RADIUS server. If the RADIUS server cannot be reached, then no authenication method is used. However, if a failure occured, the port remains unauthorized and access is not granted.

RADIUS — Indicates that authentication occurs at the RADIUS server.

None — Indicates that no authentication method is used.

Interface — Contains a list of interfaces to authenticate.

User Name — The user name as configured in the RADIUS server.

Admin Interface Control — Defines the port authorization state. The possible field values are:

Auto — Enables port based authentication per port. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.

Authorized — Places the interface into an authorized state without being authenticated. The interface sends and receives normal traffic without client port based authentication.

Unauthorized — Denies the selected interface system access by moving the interface into unauthorized state. The device cannot provide authentication services to the client through the interface.

Current Interface Control — The current port authorization state. An asterisk displays if the port is currently down.

Periodic Reauthentication — Reauthenticates the selected port periodically, when enabled.

Reauthentication Period (300-4294967295) — Indicates the time span in which the selected port is reauthenticated. The field value is in seconds. The field default is 3600 seconds.

Reauthenticate Now — Forces immediate port reauthentication, when selected.

Authentication Server Timeout (1-65535) — Defines the amount of time that lapses before the device resends a request to the authentication server. The field value is in seconds. The field default is 30 seconds.

Resending EAP Identity Request (1-65535) — Defines the amount of time that lapses before EAP requests are resent. The field value is in seconds. The field default is 30 seconds.

Quiet Period (1-65535) — Defines the amount of time that the device remains in the quiet state following a failed authentication exchange. The possible field range is 0-65535. The field value is in seconds. The field default is 60 seconds.

Supplicant Timeout (1-65535) — Defines the amount of time that lapses before EAP requests are resent to the user. The field value is in seconds. The field default is 30 seconds.

Max EAP Requests (1-10) — The maximum number of times the device can send an EAP request before restarting the authentication process if it does not receive a response. The possible field range is 1-10. The field default is 2 retries.

Displaying the Port Based Authentication Table

1. Open the **Port Based Authentication** page.
2. Click **Show All**.

   The **Port Based Authentication Table** page opens:

Figure 7-2. Port Based Authentication Table

The **Port Based Authentication Table** contains the following fields:

Copy Parameters From Port No. — The port from which parameters are copied.

Termination Cause — The reason for which the port authentication was terminated.

Copy To — Copies port parameters from one port to the selected ports.

Select All — Selects all ports in the **Port Based Authentication Table**.

Copying Parameters in the Port Based Authentication Table

1. Open the **Port Based Authentication** page.
2. Click **Show All**.

   The **Port Based Authentication Table** opens.
3. Select the interface in the **Copy Parameters from** field.
4. Select the **Copy to** check box to define the interfaces to which the Port based authentication parameters are copied.

5 Click **Apply Changes**.

The parameters are copied to the selected port in the **Port Based Authentication Table**, and the device is updated.

Enabling Port Based Authentication Using the CLI Commands

The following table summarizes the equivalent CLI commands for enabling port based authentication as displayed in the **Port Based Authentication** page.

Table 7-1. Port Authentication CLI Commands

CLI Command	Description
`aaa authentication dot1x default` *`method1`* `[`*`method2.`*`]`	Specifies one or more authentication, authorization, and accounting (AAA) methods for use on interfaces running IEEE 802.1X.
`dot1x system-auth-control`	Enables 802.1X globally.
`dot1x port-control {auto | force-authorized | force-unauthorized}`	Manually controls the authorization state of the port.
`dot1x max-req` *`count`*	Sets the maximum number of times that the device sends an EAP to the client, before restarting the authentication process.
`dot1x re-authenticate [ethernet` *`interface`*`]`	Manually initiates a re-authentication of all 802.1X-enabled ports or the specified 802.1X-enabled port.
`dot1x re-authentication`	Enables periodic re-authentication of the client.
`dot1x timeout quiet-period` *`seconds`*	Sets the number of seconds that the device remains in the quiet state following a failed authentication exchange.
`dot1x timeout re-authperiod` *`seconds`*	Sets the number of seconds between re-authentication attempts.
`dot1x timeout server-timeout` *`seconds`*	Sets the time for the retransmission of packets to the authentication server.
`dot1x timeout supp-timeout` *`seconds`*	Sets the time for the retransmission of an EAP request frame to the client.

Table 7-1. Port Authentication CLI Commands

CLI Command	Description
`dot1x timeout tx-period` *seconds*	Sets the number of seconds that the device waits for a response to an EAP - request/identity frame, from the client, before resending the request.
`show dot1x [ethernet` *interface*`]`	Displays 802.1X status for the device or for the specified interface.
`show dot1x users [username` *username*`]`	Displays 802.1X users for the device.
`show dot1x statistics ethernet` *interface*	Displays 802.1X statistics for the specified interface.

The following is an example of the CLI commands:

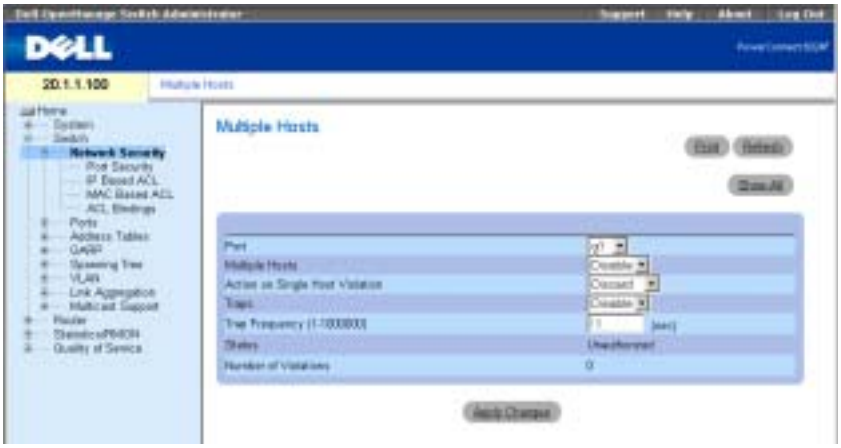
```
Console# show dot1x

Port   Admin Mode   Oper Mode      Reauth     Reauth    Username
                                   Control    Period
----   ----------   ----------     -------    ------    --------
g11    Auto         Authorized     Ena        3600      Bob
g12    Auto         Authorized     Ena        3600      John
g13    Auto         Unauthorized   Ena        3600      Clark
g14    Force-auth   Authorized     Dis        3600      n/a
```

Configuring Advanced Port Based Authentication

The **Multiple Hosts** page provides information for defining advanced port based authentication settings for specific ports.

To open the **Multiple Hosts** page, click **Switch** →**Network Security** →**Multiple Hosts**.

Figure 7-3. Multiple Hosts



The **Multiple Hosts** page contains the following fields:

Port — The port number for which Advanced Port Based Authentication is enabled.

Multiple Hosts — Enables or disables a single host to authorize multiple hosts for system access. This setting must be enabled in order to either disable ingress filtering, or to use port-lock security on the selected port.

Action on Single Host Violation — Defines the action to be applied to packets arriving in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address. The possible field values are:

Forward — Forwards the packets from an unknown source, however, the MAC address is not learned.

Discard — Discards the packets from any unlearned source. This is the default value.

Discard Shutdown — Discards the packet from any unlearned source and shuts down the port. Ports remain shut down until they are activated, or the device is reset.

Traps — Enables or disables sending traps to the host if a violation occurs.

Trap Frequency (1-1000000) — Defines the time period by which traps are sent to the host. The default is 10 seconds.

Status — The host status. The possible field values are:

Unauthorized — Indicates that the port control is *Force Unauthorized*, the port link is down or the port control is Auto, but a client has not been authenticated via the port.

Not in auto mode — Indicates that the port control is *Forced Authorized*, and clients have full port access.

Single-host Lock — Indicates that the port control is *Auto* and a single client has been authenticated via the port.

No Single Host — Indicates that Multiple Host is enabled.

Number of Violations — The number of packets that arrived on the interface in single-host mode, from a host whose MAC address is not the client (supplicant) MAC address.

Displaying the Multiple Hosts Table

1. Open the **Multiple Hosts** page.
2. Click **Show All**.

   The **Multiple Hosts Table** opens.

Figure 7-4. Multiple Hosts Table

Enabling Multiple Hosts Using the CLI Commands

The following table summarizes the equivalent CLI commands for enabling the advanced port based authentication as displayed in the **Multiple Hosts** page.

Table 7-2. Multiple Hosts CLI Commands

CLI Command	Description
`dot1x multiple-hosts`	Allows multiple hosts (clients) on an 802.1X-authorized port that has the dot1x port-control interface configuration command set to auto.

Table 7-2. Multiple Hosts CLI Commands

CLI Command	Description
`dot1x single-host-violation {forward |discard |discard-shutdown}[trap` *`seconds`*`]`	Configures the action to be taken when a station, whose MAC address is not the client (supplicant) MAC address, attempts to access the interface.

The following is an example of the CLI Command.

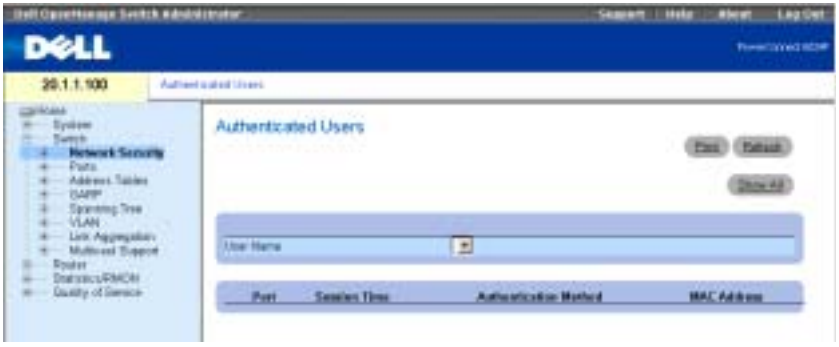
```
Console(config)# interface ethernet g11
Console(config-if)# dot1x multiple-hosts
```

Authenticating Users

The **Authenticated Users** page displays user port access lists.

To open the **Authenticated Users** page, click **Switch** →**Network Security** →**Authenticated Users**.

Figure 7-5. Authenticated Users



The **Authenticated Users** page contains the following fields:

User Name — List of users authorized via the RADIUS Server.

Port — Lists the port numbers used for authentication. The ports are listed by user name.

Session Time — The amount of time the user was logged on to the device. The field format is **Day:Hour:Minute:Seconds**, for example, 3 days: 2 hours: 4 minutes: 39 seconds.

Authentication Method — The method by which the last session was authenticated. The possible field values are:

Remote — The user was authenticated from a remote server.

None — The user was not authenticated.

MAC Address — The supplicant MAC address.

Displaying the Authenticated Users Table

1. Open the **Authenticated Users** page.
2. Click **Show All**.

   The **Authenticated Users Table** opens:

Figure 7-6. Authenticated Users Table

Displaying Authenticating Users Using the CLI Commands

The following table summarizes the equivalent CLI commands for authenticating users as displayed in the **Authenticated Users** page.

Table 7-3. Add User Name CLI Commands

CLI Command	Description
`show dot1x users [username` *`username`*`]`	Displays 802.1X users for the device.

The following is an example of the CLI commands:

```
Console# show dot1x users
Port     Username   Session Time   Auth Method   MAC Address
----     --------   ------------   -----------   -----------------
g12      bob        00:09:27       Remote        00:80:c8:b9:dc:1d
```

Configuring Port Security

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. The MAC addresses can be dynamically learned, up to that point, or they can be statically configured. Locked port security monitors both received and learned packets that are received on specific ports. Access to the locked port is limited to users with specific MAC addresses. These addresses are either manually defined on the port, or learned on that port up to the point when it is locked. When a packet is received on a locked port, and the packet's source MAC address is not tied to that port (either it was learned on a different port, or is unknown to the system), the

protection mechanism is invoked, and can provide various options. Unauthorized packets arriving to a locked port are either forwarded, discarded with no trap, discarded with a trap or the ingress port is disabled.

Locked port security also enables storing a list of MAC addresses in the configuration file. The MAC address list can be restored after the device has been reset.

Disabled ports can only be activated from the **Port Configuration** page.

To open the **Port Security** page, select **Switch→Network Security→Port Security**.

Figure 7-7. Port Security

Interface — Indicates whether locked port security is enabled on a port or LAG.

Current Port Status — Indicates if the port is currently locked and disabled, or if it is unlocked.

Set Port — Enables locking the port. When a port is locked, all the current addresses that had been dynamically learned by the switch on that port, are transformed to static MAC addresses. When the port is unlocked, they are removed from the static list.

Action on Violation — Action applied to packets arriving on the port. The field is grayed if the port is unlocked. Possible values are:

Discard — Discards the packets from any unlearned source. This is the default value.

Forward — Forwards the packets from an unknown source. The MAC address is not learned.

Shutdown — Discards the packet from any unlearned source and sends a trap. In addition, the ingress port is disabled.

Trap — Enables or disables sending a trap when a packet is received on a locked port.

Trap Frequency — Amount of time (seconds) between traps.

Defining a Locked Port

1. Open the **Port Security** page.
2. Select an interface type and number.
3. Select **Locked** on the **Set Port** drop-down menu.
4. Complete the remaining fields.
5. Click **Apply Changes**.

   The locked port is added to the Port Security table, and the device is updated.

Copying Parameters in the Locked Port Table

1. Open the **Port Security** page.
2. Click **Show All to display** the **Port Security Table**.

   The fields in the Port Security Table are the same as the fields in the **Port Security** page.
3. In the **Copy Parameters from** field, select an interface in either the **Port** or **LAG** drop-down menu.

   The port security definitions for this interface are copied to the selected interfaces, see step 5.
4. Check the **Copy to** check box to select the interfaces to which the port security definitions are copied.

   Or

   Click **Select All** to copy the definitions to all ports or LAGs.
5. Click **Apply Changes**.

   The parameters are copied to the selected port ports or LAGs in the **Port Security Table**, and the device is updated.

Configuring Locked Port Security with CLI Commands

The following table summarizes the equivalent CLI commands for configuring locked port security as displayed in the **Port Security** page.

Table 7-4. Locked Port Security CLI Commands

CLI Command	Description
`port security [forward | discard | discard-shutdown] [trap` *`seconds`*`]`	Disables new address learning on an interface.
`show ports security [ethernet` *`interface`* `| port-channel port-` *`channel-number`*`]`	Displays the port-lock status.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g1
Console(config-if)# port security forward trap 100
Console(config-if)# exit
Console(config)# exit
Console# show ports security
Port       status     Action     Trap       Frequency  Counter
----       ------     ------     ----       ---------  -------
g1         Locked     Forward    Enabled    100        0
g2         Unlocked   -          -          -          -
...
g24        Unlocked   -          -          -          -
ch1        Unlocked   -          -          -          -
...
ch7        Unlocked   -          -          -          -
```

Defining IP based ACLs

Access control lists (ACL) allow network managers to define classification actions and rules for specific ingress ports. Your switch supports up to 1,024 ACLs. Packets entering an ingress port, with an active ACL, are either admitted or denied entry and the ingress port is disabled. If they are denied entry, the user can disable the port.

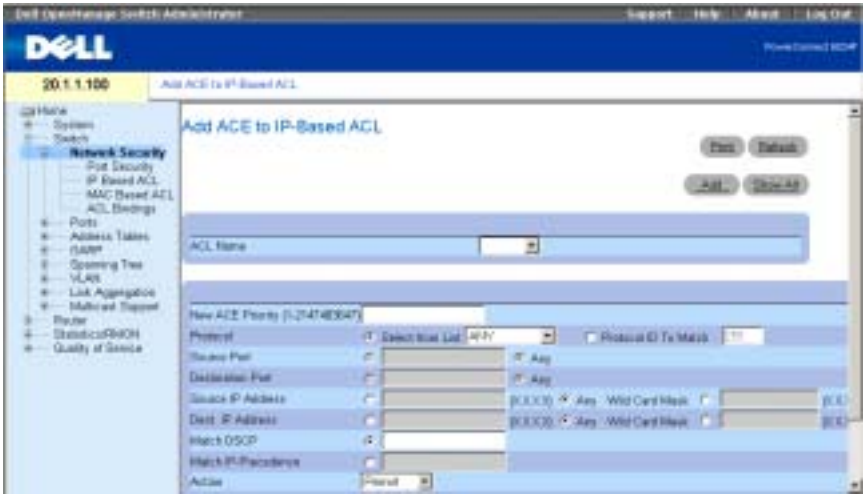
For example, a network administrator defines an ACL rule that says, port number 20 can receive TCP packets, however, if a UDP packet is received, the packet is dropped.

ACLs are composed of access control entries (ACEs) that are made of the filters that determine traffic classifications. The total number of ACEs that can be defined in all ACLs together is 1024.

Use the **Add ACE to IP Based ACL** page to define IP-based ACEs.

To open the **Add ACE to IP Based ACL** page, select **Switch→Network Security→IP Based ACL**.

Figure 7-8. Add ACE to IP Based ACL



The **Add ACE to IP Based ACL** page contains the following fields:

ACL Name — User-defined ACLs.

New ACE Priority — ACE priority that determines which ACE is matched to a packet based on a first-match basis.

Protocol — Enables creating an ACE based on a specific protocol.

Select from List — Click to select from a protocols list on which ACE can be based.

Protocol ID To Match— Click to add a user-defined protocol by which packets are matched to the ACE.

NOTE: Using "any" specifies that all IP protocols are selected.

Source Port— The TCP/UDP source port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu.

Destination Port— The TCP/UDP destination port. This field is active only if **800/6-TCP** or **800/17-UDP** are selected in the **Select from List** drop-down menu.

Source IP Address—Matches the source port IP address to which packets are addressed to the ACE.

Wild Card Mask — Source IP address wildcard mask.Wild card masks specify which bits are used and which bits are ignored. A wild card mask of 255.255.255.255 indicates that no bit is important. A wildcard of 0.0.0.0 indicates that all the bits are important.

Dest. IP Address — Matches the destination port IP address to which packets are addressed to the ACE.

Wild Card Mask — The Destination IP address wildcard mask. Select either **Match DSCP** or **Match IP Precedence**:

Match DSCP — Matches the packet DSCP value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.

Match IP Precedence — Matches the packet IP Precedence value to the ACE. Either the DSCP value or the IP Precedence value is used to match packets to ACLs.

Action — The ACL forwarding action. Possible values are:

Permit — Forwards packets which meet the ACL criteria.

Deny — Drops packets which meet the ACL criteria.

Shutdown — Drops packet that meets the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the **Ports Configuration** page, see "Defining Port Configuration."

To see all the ACEs attached to the ACE, click **Show All**.

Adding an IP based ACL

1. Open the **Add ACE to IP Based ACL** page.
2. Click **Add** to display the **Add IP Based ACL** page.

Figure 7-9. Add IP Based ACL

3. Enter the **ACL Name**.
4. Check the **New ACE Priority** check box and define all of the fields in the page.
5. Click **Apply Changes**.

   The IP based ACL is defined, and the device is updated.

Modifying an IP based ACE

NOTE: ACEs can be modified only when the ACL to which they belong is not bound to an interface.

1. Open the **Add ACE to IP Based ACL** page.
2. Click **Show All** to display all ACEs in the ACL.
3. Select an ACL in the **ACL Name** field.
4. Modify the fields as desired.
5. Click **Apply Changes**.

   The IP-based ACE is modified, and the device is updated.

Adding New ACEs to an IP-Based ACL

1. Open the **Add ACE to IP Based ACL** page.
2. Select an ACL in the **ACL Name** field.
3. Define the fields in the dialog.
4. Click **Apply Changes**.

   The ACE is assigned to the IP based ACL.
5. Click Apply Changes and fill in the new ACE's parameters to additional ACEs to an existing ACL

Reordering ACEs in an ACL

1. Open the **Add ACE to IP Based ACL** page, and select the ACL to be operated upon from the **ACL Name** drop-down menu.
2. Click **Show All**.

   The **ACEs Associated with IP-ACL** page opens.
3. Enter a priority number that orders the ACE as desired.
4. Click **Apply Changes**.

   The ACE is reordered and the device is updated.

Removing ACLs

1. Open the **Add ACE to IP Based ACL** page, and select the ACL to be operated upon from the **ACL Name** drop-down menu.
2. Click **Show All**.

   The **ACEs Associated with IP-ACL** page opens.
3. Check the **Remove ACL** check box
4. Click **Apply Changes**.

The IP based ACL is removed, and the device is updated.

Assigning IP based ACEs to ACLs Using the CLI Commands

The following table summarizes the equivalent CLI commands for assigning IP based ACEs to ACLs as displayed in the **Add ACE to IP Based ACL** page.

Table 7-5. IP Based ACEs to ACLs CLI Commands

CLI Command	Description
`ip access-list` *name*	Creates IP ACLs and enters IP Access-list configuration mode.
`permit {any |` *protocol*`} {any | source` *source-wildcard*`} {any | destination` *destination-wildcard*`} [dscp` *dscp number* `| ip-precedence` *ip-precedence*`]`	Allows traffic if the conditions defined in the permit statement are matched.
`deny [disable-port] {any |` *protocol*`} {any | source` *source-wildcard*`} {any | destination` *destination-wildcard*`} [dscp` *dscp number* `| ip-precedence` *ip-precedence*`]`	Denys traffic if the conditions defined in the deny statement are matched.
`show access-lists [`*name*`]`	Displays Access Control Lists defined on the switch.

The following is an example of the CLI commands:

```
Console(config)# ip access-list Dell
Console(config-ip-al)# permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
Console(config-ip-al)# deny any 192.1.1.10 0.0.0.255 any
Console# show access-lists
IP access list one
permit ip host 12.1.1.1 any
permit rsvp host 176.30.40.1 any
Console# show access-lists
IP access list Dell
permit rsvp 12.1.1.1 0.0.0.0 any dscp 56
deny any 192.1.1.10 0.0.0.255 any
```

Defining MAC based ACLs

The **Add ACE to MAC Based ACL** page allows network administrators to define a MAC- based ACL. For an explanation of ACLs, see "Defining IP based ACLs."

To open the **Add ACE to MAC Based ACL** page, select **Switch→Network Security→MAC based ACL**.

Figure 7-10. Add ACE to MAC Based ACL

The **Add ACE to MAC Based ACL** page contains the following fields:

ACL Name — User-defined ACL.

New ACE Priority — ACE priority, which determines which ACE is matched to a packet on a first-match basis.

Source MAC Address—Matches the source MAC address from which packets are addressed to the ACE.

Wild Card Mask — The source MAC address wildcard mask. Wild cards are used to mask all or part of a source MAC address. Wild card masks specify which bits are used and which bits are ignored. A wild card mask of FF:FF:FF:FF:FF:FF indicates that no bit is important. A wildcard of 00.00.00.00.00.00 indicates that all the bits are important.
For example, if the source MAC address E0:3B:4A:C2:CA:E2 and the wildcard mask is 00:3B:4A:C2:CA:FF, the first two bits of the MAC are used, while the last two bits are ignored.

Destination MAC Address — Matches the destination MAC address to which packets are addressed to the ACE.

Wild Card Mask — The destination MAC address wildcard mask. Wild cards are used to mask all or part of a destination MAC address.

VLAN ID — Matches the packet's VLAN ID to the ACE. The possible field values are 1-4094.

Action — Indicates the ACL forwarding action. Possible field values are:

Permit — Forwards packets which meet the ACL criteria.

Deny — Drops packets which meet the ACL criteria.

Shutdown — Drops packet that meet the ACL criteria, and disables the port to which the packet was addressed. Ports are reactivated from the **Ports Configuration** page, see "Defining Port Configuration."

Adding a MAC-Based ACL

1. Open the **Add ACE to MAC Based ACL** page.
2. Click **Add** to open the **Add MAC Based ACL** page.

Figure 7-11. Add MAC Based ACL

3. Enter the **ACL Name**.
4. To add a new ACE to the newly created ACL, check the **New ACE Priority** check box and define the **Source** and **Destination** MAC addresses, **VLAN ID** and **Action** fields.
5. Click **Apply Changes**.

   The MAC-based ACL is defined, and the device is updated.

Modifying a MAC based ACE

1. Open the **Add ACE to MAC Based ACL** page.
2. Select an ACL in the **ACL Name** field.
3. Modify the required fields.
4. Click **Apply Changes**.

   The fields are modified, and the device is updated.

Adding ACEs to a MAC based ACL

NOTE: ACEs can be added only if the ACL is not bound to an interface.

1. Open the **Add ACE to MAC Based ACL** page.
2. Select an ACL in the **ACL Name** field.
3. Define the **New ACE Priority**, **Source** and **Destination** MAC addresses, **VLAN ID** and **Action** fields.
4. Click **Apply Changes**.

   The ACE is assigned to the MAC-based ACL.

NOTE: To add more than one ACE to an existing ACL, click **Apply Changes** and fill in the new ACE's parameters.

Displaying ACL-Specific ACEs

1. Open the **Add ACE to MAC Based ACL** page.
2. Click **Show All** to display the **ACEs Associated with MAC ACL** page.

Removing ACLs

NOTE: ACLs can be removed only if they are not bound to an interface.

1. Select an ACL.
2. Open the **Add ACE to MAC Based ACL** page.
3. Click **Show All** to display the **ACEs Associated with MAC ACL** page.
4. Check the **Remove ACL** check box.
5. Click **Apply Changes**.

   The MAC-based ACL is removed, and the device is updated.

Removing ACEs From an ACL

1. Select an ACL.
2. Open the **Add ACE to MAC Based ACL** page.
3. Click **Show All** to display the **ACEs Associated with MAC ACL** page.
4. Check the **Remove ACE** check box in the row of the ACE to be removed.
5. Click **Apply Changes**.

   The MAC-based ACL is removed, and the device is updated.

Assigning MAC based ACEs to ACLs Using the CLI Commands

The following table summarizes the equivalent CLI commands for assigning MAC based ACEs to ACLs as displayed in the **Add ACE to MAC Based ACL** page.

Table 7-6. MAC-Based ACE CLI Commands

CLI Command	Description
`mac access-list` *name*	Creates Layer 2 MAC ACLs, and enters to MAC-Access list configuration mode.
`permit {any | host source` *source-wildcard*`} {any | destination` *destination-wildcard*`}[vlan` *vlan-id*`]`	Allows traffic if the conditions defined in the permit statement are matched.
`deny [disable-port] {any | source` *source-wildcard*`} {any | destination` *destination-wildcard*`}[vlan` *vlan-id*`]`	Denies traffic if the conditions defined in the deny statement are matched.
`show access-lists [`*name*`]`	Displays Access Control Lists configured on the switch.

The following is an example of the CLI commands:

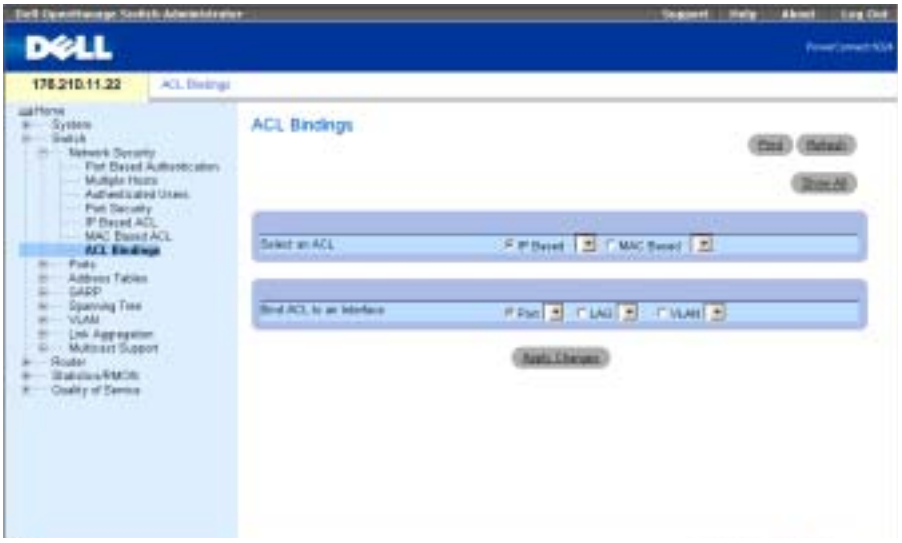
```
Console(config)# mac access-list dell

Console(config-mac-al)# permit 6:6:6:6:6:6 0:0:0:0:0:0 any vlan 4

Console(config-mac-al)# deny 6:6:6:6:6:6 0:0:255:255:255:255
```

Configuring ACL Binding

When an ACL is bound to an interface, all the ACE rules that have been defined are applied to the selected interface. Use the **ACL Bindings** page to assign ACL lists to classification methods and interfaces.

To open the **ACL Bindings** page, select **Switch→Network Security→ACL Binding**.

Figure 7-12. ACL Bindings



The **ACL Bindings** page contains the following fields:

Select an ACL — The ACL type to which incoming packets are matched. Packets can be matched to either IP based ACLs or MAC Address based ACLs.

Bind ACL to Interface — The interface and interface type to which the ACL is attached. You can attach the ACL to a port, LAG, or VLAN.

Assigning an ACL to an Interface

1. Open the **ACL Bindings** page.
2. Select the ACL type in the **Select ACL** field.
3. Select the interface to which the ACL is attached in the **Bind ACL to an Interface** field.

NOTE: Whenever an ACL is assigned on a port, LAG or, VLAN, flows from that ingress interface that do not match the ACL are matched to the default rule, which is Drop unmatched packets.

4. Click **Apply Changes**.

   The ACL is attached to the interface.

Removing an Entry from the ACL Bindings Table

1. Open the **ACL Bindings** page.
2. Click **Show All** to display the **ACL Bindings Table**.
3. Check the **Remove** check box for the entry that you want to remove.

4 Click **Apply Changes**.

The selected entry is removed from the table, and the device is updated.

Displaying the ACL Bindings Table

1 Open the **ACL Bindings** page.

2 Click **Show All** to display the **ACL Bindings Table**.

The fields in the **ACL Bindings Table** are the same as the fields on the **ACL Bindings** page.

Copying Parameters in the ACL Bindings Table

1 Open the **ACL Bindings** page.

2 Click **Show All** to display the **ACL Bindings Table**.

3 Select an interface in the **Copy Parameters from** field.

4 Select a port/trunk in the **Port/LAG** or **VLAN** drop-down menu.

The definitions for this interface will be copied to the selected target ports/trunks.

5 Check the **Copy to** check box for the entry to be edited, or to copy the definitions to all available ports/trunks, click **Select All**.

6 Click **Apply Changes**.

The parameters are copied to the target ports/trunks in the *ACL Bindings Table*, and the device is updated.

Assigning ACL Membership Using the CLI Commands

The following table summarizes the equivalent CLI commands for assigning ACL membership as displayed in the **ACL Bindings** page.

Table 7-7. ACL Binding CLI Commands

CLI Command	Description
`class-map class-map-name [match-all | match-any]`	Creates class maps and enters the class-map configuration mode.
`match access-group` *`acl-name`*	Defines the match criterion to classify traffic.
`show class-map [`*`class-map-name`*`]`	Displays all the class maps configured on the device.

The following is an example of the CLI commands:

```
Console (config)# class-map class1 match-all
Console (config-cmap)# match access-group dell
```

```
Console (config-cmap)# exit
Console (config)# exit
Console> exit
Console> show class-map class1
Class Map match-all class1 (id4)
```

Configuring Ports

The **Ports** page provides links for configuring port functionality including advanced features such as storm control and port mirroring, and for performing virtual port tests.

To open the **Ports** page Select **Switch→Ports**.

Defining Port Configuration

Use the **Port Configuration** page to define port parameters.

To open the **Port Configuration** page, click **Switch→Ports→Port Configuration** in the tree view.

Figure 7-13. Port Configuration

The **Port Configuration** page contains the following fields:

Port — The port number for which port parameters are defined.

Description (0-64 Characters)— A brief interface description, such as Ethernet.

Port Type — The type of port.

Admin Status — Enables or disables traffic forwarding through the port.

Current Port Status — Specifies whether the port is currently operating or non-operational.

Reactivate Suspended Port — Reactivates a port if the port has been disabled through the locked port security option.

Operational Status — Indicates the port operational status. Possible field values are:

Suspended — The port is currently active, and is currently not receiving or transmitting traffic.

Active — The port is currently active and is currently receiving and transmitting traffic.

Disable — The port is currently disabled, and is not currently receiving or transmitting traffic.

Admin Speed — The configured rate for the port. The port type determines what speed setting options are available. You can designate admin speed only when the port is disabled.

Current Port Speed — The actual synchronized port speed (bps).

Admin Duplex — The port duplex mode in bps. **Full** indicates that the interface supports transmission between the device and the client in both directions simultaneously. **Half** indicates that the interface supports transmission between the device and the client in only one direction at a time.

Current Duplex Mode — The synchronized port duplex mode.

Auto Negotiation — Enables Auto Negotiation on the port.
Auto Negotiation is a protocol between two link partners that enables a port to advertise its transmission rate, duplex mode and flow control abilities to its partner.

Current Auto Negotiation — The current Auto Negotiation setting.

Admin Advertisement — Specifies the capabilities to be advertised by the port. The possible field values are:

Max Capability - Indicates that all port speeds and Duplex mode settings can be accepted.

10 Half - Indicates that the port is advertising a 10 mbps speed and half Duplex mode setting.

10 Full - Indicates that the port is advertising a 10 mbps speed and full Duplex mode setting.

100 Half - Indicates that the port is advertising a 100 mbps speed and half Duplex mode setting.

100 Full- Indicates that the port is advertising a 100 mbps speed and full Duplex mode setting.

1000 Full- Indicates that the port is advertising a 1000 mbps speed and full Duplex mode setting.

Current Advertisement — The port advertises its speed to its neighbor port to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.

Neighbor Advertisement — The neighbor port (the port to which the selected interface is connected) advertises its capabilities to the port to start the negotiation process. The possible values are those specified in the **Admin Advertisement** field.

Back Pressure — Enables Back Pressure mode on the port. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages. Back Pressure is not supported in Out-of-Band ports.

Current Back Pressure — The current Back Pressure setting.

Flow Control — Enables or disables flow control or enables the auto negotiation of flow control on the port.

Current Flow Control — The current Flow Control setting.

MDI/MDIX — Allows the device to decipher between crossed and uncrossed cables.

Hubs and switches are deliberately wired opposite the way end stations are wired, so that when a hub or switch is connected to an end station, a straight through Ethernet cable can be used, and the pairs are match up properly. When two hubs/switches are connected to each other, or two end stations are connected to each other, a crossover cable is used ensure that the correct pairs are connected. Auto MDIX does not operate on FE ports if auto negotiation is disabled. MDIX is not supported in Out-of-Band ports.

Possible values are:

Media Dependent Interface with Crossover (MDIX) — Use for hubs and switches.

Media Dependent Interface (MDI) — Use for end stations.

Current MDI/MDIX—Indicates the current device MDIX settings. Possible field values are:

MDI — The current MDI setting is MDI.

MDIX — The current MDI setting is MDIX.

Auto — The value is set automatically.

LAG—Specifies if the port is part of a LAG.

PVE— Enables a port as a Private VLAN Edge (PVE) port. When a port is defined as PVE, it bypasses the Forwarding Database (FDB), and forwards all Unicast, Multicast and Broadcast traffic to an uplink (except MAC-to-me packets). Uplinks can be a port or LAG. Traffic from the uplink is distributed to all interfaces.

Defining Port Parameters

1. Open the **Port Configuration** page.
2. Select a port in the **Port** Field.
3. Define the available fields in the dialog.
4. Click **Apply Changes**.

   The port parameters are saved to the device.

Displaying the Port Table

1. Open the **Port Configuration** page.
2. Click **Show All** to display the **Port Configuration Table**.

Configuring Ports with CLI Commands

The following table summarizes the equivalent CLI commands for configuring ports as displayed in the **Port Configuration** page.

Table 7-8. Port Configuration CLI Commands

CLI Command	Description
`interface ethernet` *`interface`*	Enters the interface configuration mode to configure an ethernet type interface.
`description` *`string`*	Adds a description to an interface configuration.
`shutdown`	Disables interfaces that are part of the currently set context.
`set interface active {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Reactivates an interface that is shutdown due to security reasons.
`speed {10 | 100 | 1000}`	Configures the speed of a given ethernet interface when not using auto negotiation.
`duplex {half | full}`	Configures the full/half duplex operation of a given ethernet interface when not using auto negotiation.
`negotiation`	Enables auto negotiation operation for the speed and duplex parameters of a given interface.
`back-pressure`	Enables Back Pressure on a given interface.
`flowcontrol {auto | on | off}`	Configures the Flow Control on a given interface.
`mdix {on | auto}`	Enables automatic crossover on a given interface or Port-channel.

Table 7-8. Port Configuration CLI Commands

CLI Command	Description
`show interfaces configuration [ethernet` *`interface`* `| port-channel` *`port-channel-number`* `oob-eth` *`interface`*`]`	Displays the configuration for all configured interfaces.
`show interfaces status [ethernet` *`interface`* `| port-channel` *`port-channel-number`* `oob-eth` *`interface`*`]`	Displays the status for all configured interfaces.
`show interfaces description [ethernet` *`interface`* `| port-channel` *`port-channel-number`* `oob-eth` *`interface`*`]`	Displays the description for all configured interfaces.

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g18
Console (config-if)# description RD_SW#3
Console(config-if)# speed 100
Console (config-if)# shutdown
Console (config-if)# no shutdown
Console (config-if)# duplex full
Console (config-if)# negotiation
Console (config-if)# back-pressure
Console (config-if)# flowcontrol on
Console (config-if)# mdix auto
Console (config-if)# exit
Console (config)# exit
Console> set interface active ethernet g9
```

```
Console> show interfaces status

                                        Flow  Link     Back     Mdix
Port  Type      Duplex  Speed  Neg      ctrl  State    Pressure Mode
---   ------    ----    ---    ---      ----- -----    -----    -----
g1    1G-       Full    1000   Enabled  Off   Up       Disabled Off
      Copper
g2    1G-       Full    1000   Enabled  Off   Up       Disabled Off
      Copper
g3    1G-       Full    1000   Enabled  Off   Up       Disabled Off
      Copper


                                          Flow       Link       Back
Ch    Type      Duplex     Speed    Neg    control    State      Pressure
---   --------  -----      ----     ----   ------     ------     -------
ch1   Unknown   Unknown             Unknown Off        Not        Unknown
                                                     Present
ch2   Unknown   Unknown             Unknown Off        Not        Unknown
                                                     Present
ch3   Unknown   Unknown             Unknown Off        Not        Unknown
                                                     Present
ch4   Unknown   Unknown             Unknown Off        Not        Unknown
                                                     Present
Console# show interfaces configuration

                                          Flow       Admin    Back
Ch    Type       Duplex    Speed   Neg    control    State    Pressure
---   -------    ---       ---     ----   -------    -----    --------
ch1   Unknown                     Enable Off        Up       Disabled
                                  d
ch2   Unknown                     Enable Off        Up       Disabled
                                  d
```

```
ch3    Unknown                    Enable Off        Up       Disabled
                                  d

            Console# show interfaces description ethernet 1

Port  Description
----- -----------------
g1    connect_to_server
```

Defining LAG Configuration

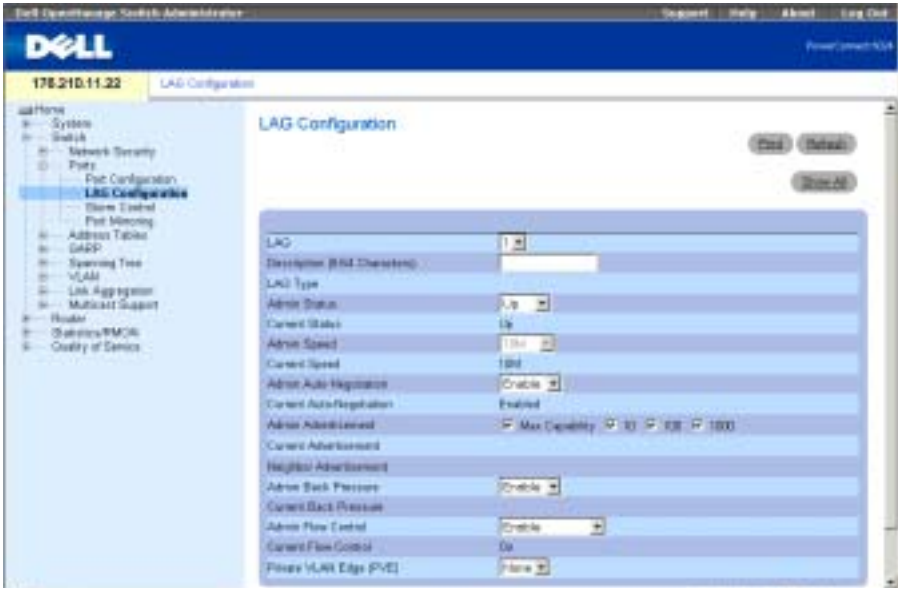
Multilayer switches support the bundling of several links into a single logical link of aggregate capacity called a link aggregrated group (LAG). LAGs are often called trunks or aggregate links.

Use the **LAG Configuration** page to configure LAGs parameters. Your switch supports up to seven ports per LAG, and seven LAGs per system. If port configuration is modified while a port is a LAG member, the configuration change is only effective after the port is removed from the LAG.

For information about Aggregating Ports and assigning ports to LAGs, see "Aggregating Ports."

To open the **LAG Configuration** page, click **Switch→Ports→LAG Configuration** in the tree view.

Figure 7-14. LAG Configuration



The **LAG Configuration** page contains the following fields:

LAG — Contains a list of LAG numbers.

Description (0-64 Characters)— Description of the port.

LAG Type — The port types that comprise the LAG.

Admin Status — Enables or disables traffic forwarding through the selected LAG.

Current Status — Indicates if the LAG is currently operating.

Admin Speed — The speed at which the LAG is operating.

Current Speed — The current speed at which the LAG is operating.

Admin Auto Negotiation — Enables or disables Auto Negotiation on the LAG. Auto-negotiation is a protocol between two link partners that enables a LAG to advertise its transmission rate, duplex mode and flow control (the flow control default is disabled) abilities to its partner.

Current Auto Negotiation — The current Auto Negotiation setting.

Admin Advertisement — Specifies the capabilities to be advertised by the LAG. The possible field values are:

Max Capability - Indicates that all LAG speeds and Duplex mode settings can be accepted.

10 - Indicates that the LAG is advertising a 10 mbps speed and full Duplex mode setting.

100 - Indicates that the LAG is advertising a 100 mbps speed and full Duplex mode setting.

1000 - Indicates that the LAG is advertising a 1000 mbps speed and full Duplex mode setting.

Current Advertisement — The LAG advertises its capabilities to its neighbor LAG to start the negotiation process. The possible field values are those specified in the **Admin Advertisement** field.

Neighbor Advertisement — The neighbor LAG (the LAG to which the selected interface is connected) advertises its capabilities to the LAG to start the negotiation process. The possible values are those specified in the **Admin Advertisement** field.

Admin Back Pressure — Enables or disables Back Pressure mode on the device. Back Pressure mode is used with Half Duplex mode to disable ports from receiving messages.

Current Back Pressure — Indicates if Back Pressure mode is enabled or disabled.

Admin Flow Control — Enables or disables flow control or enables the auto negotiation of flow control on the LAG.

Current Flow Control — The user-designated Flow Control setting.

Defining LAG Parameters

1. Open the **LAG Configuration** page.
2. Select a LAG in the **LAG** field.
3. Define the available fields.

4 Click **Apply Changes**.

The LAG parameters are saved to the device.

Displaying the LAG Configuration Table

1 Open the **LAG Configuration** page.

2 Click **Show All** to display the **LAG Configuration Table**.

Configuring LAGs with CLI Commands

The following table summarizes the equivalent CLI commands for configuring LAGs as displayed in the **LAG Configuration** page.

Table 7-9. LAG Configuration CLI Commands

CLI Command	Description
`interface port-channel` *`port-channel-number`*	Enters the interface configuration mode of a specific port-channel.
`channel-group` *`port-channel-number`* `mode {on | auto}`	Associates a port with a Port-channel.
`show interfaces port-channel [`*`port-channel-number`*`]`	Displays Port-channel information (which ports are members of that port-channel, and whether they are currently active or not).

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g5
Console (config-if)# channel-group 1 mode on
Console (config-if)# exit
Console# show interfaces port-channel
Channel Port
-----------------------------------------------
 Ch 1 Active   g1, g2, g5  Inactive g3
 Ch 2 Active   g2
 Ch 3 Inactive g8
```

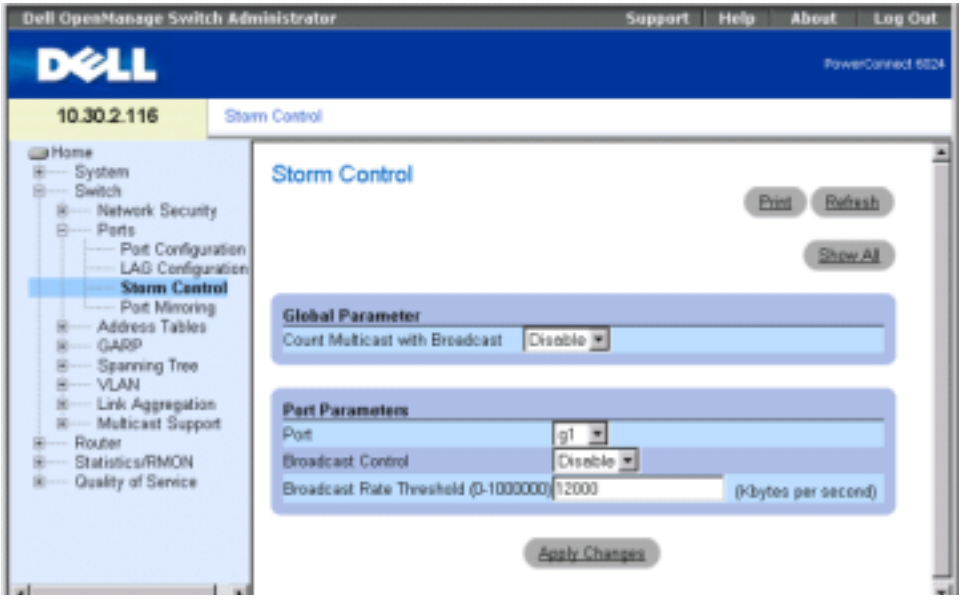
Enabling Storm Control

A broadcast storm is the result of an excessive amount of broadcast messages simultaneously transmitted across a network by a single port. Forwarded message responses can overload network resources and/or cause the network to time out.

Your switch measures the incoming broadcast/multicast packet rate per port and discards packets when the rate exceeds the defined value. Storm control is enabled per device, by defining the packet type and the rate the packets are transmitted. Ports groups provide storm protection for an entire port group.

Use the **Storm Control** page to enable and configure storm control. To open the **Storm Control** page, click **Switch→Ports→Storm Control** in the tree view.

Figure 7-15. Storm Control Page



Count Multicast with Broadcast — **Enable** counts Broadcast and Multicast traffic; **Disable** counts only Broadcast traffic.

Port — The port from which storm control is enabled.

Broadcast Control — Enables or disables forwarding unknown packet types on the device.

Broadcast Rate Threshold — The maximum rate (kilobytes per second) at which unknown packets are forwarded. The range is 0-148,800. The default value is 12000. All values are rounded to the nearest 64Kbps. If the field value is under 64Kbps, the value is rounded up to 64Kbps.

Modifying Storm Control Port Parameters

1. Open the **Storm Control** page.
2. Complete the fields on the page.
3. Click **Apply Changes**.

   The storm control port parameters are saved to the device.

Copying Parameters in the Storm Control Settings Table

1. Open the **Storm Control** page.
2. Click **Show All** to display the **Storm Control Settings Table**.
3. Select the port from which you want to copy settings from the **Copy Parameters from Port** field.
4. Check the **Copy to** check box to define the interfaces to which the storm control definitions are copied, or click **Select All** to copy the definitions to all ports.
5. Click **Apply Changes**.

   The parameters are copied to the selected port ports in the **Storm Control Settings Table**, and the device is updated.

Configuring Storm Control with CLI Commands

The following table summarizes the equivalent CLI commands for configuring Storm Control as displayed on the **Storm Control** page.

Table 7-10. Storm Control CLI Commands

CLI Command	Description
`port storm-control include-multicast`	Enables the device to count multicast packets together with broadcast packets.
`port storm-control broadcast enable`	Enables broadcast storm control.
`port storm-control broadcast rate` *`rate`*	Configures the maximum broadcast rate.
`show ports storm-control` *`port`*	Displays the storm control configuration.

The following is an example of the CLI commands:

```
Console(config)# port storm-control include-multicast

Console(config)# interface ethernet g1

Console(config-if)# port storm-control broadcast enable
```

```
Console(config-if)# port storm-control broadcast rate 100000
Console(config-if)# exit
Port       Broadcast and Multicast Storm Control [Kbytes/sec]
----       --------------------------------------------------
g1                    100000
g2                    Disabled
...
g24                   Disabled
```

Defining Port Mirroring Sessions

Port mirroring monitors and mirrors network traffic by forwarding copies of incoming and outgoing packets from one port to a monitoring port. Port mirroring can be used as diagnostic tool and/or debugging feature. Port mirroring also enables switch performance monitoring.

Network administrators configure port mirroring by selecting a specific port to copy all packets, and different ports from which the packets copied. Before configuring port mirroring, note the following:

- Monitored ports cannot operate faster than the monitoring port.
- Maximum number of source ports is eight.
- Only one mirroring session can be configured at a time.

The following restrictions apply to ports configured to be destination ports:

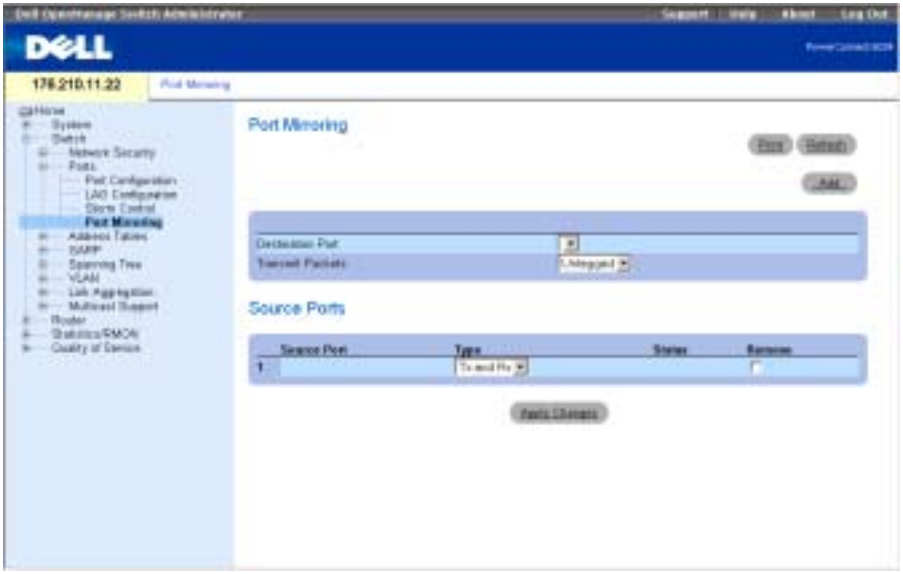
- Ports cannot be configured as a source port.
- Ports cannot be a LAG member.
- IP interfaces are not configured on the port.
- GVRP is not enabled on the port.
- The port is not a VLAN member.
- Only one destination port can be defined.

The following restrictions apply to ports configured to be source ports:

- Source Ports cannot be a LAG member.
- Ports cannot be configured as a destination port.
- All packets are transmitted tagged from the destination port.
- All the TX packets should be monitored to the same port.

To open the **Port Mirroring** page, click **Switch→Ports→Port Mirroring** in the tree view.

Figure 7-16. Port Mirroring



The **Port Mirroring** page contains the following fields:

Destination Port — Contains a list of port numbers from which port traffic may be copied.

Transmit Packets — Specifies if packets are transmitted tagged or untagged from the destination port.

Source Port — Port number to which port traffic is mirrored.

Type — Specifies the type of traffic monitored. Possible field values are:

TX — Monitors transmitted packets only.

RX — Monitors received packets only.

TX and RX — Monitors transmitted and received packets.

Status — Indicates if the port is currently monitored (**Active**) or not monitored (**Not Ready**).

Remove — When checked, removes the port mirroring session.

Adding a Port Mirroring Session

1. Open the **Port Mirroring** page.
2. Click **Add** to display the **Add Source Port** page.
3. Select the source port from the **Source Port** drop-down menu.

4 Click **Apply Changes**.

The new port mirroring session is enabled for the port, and the device is updated.

Modifying a Port Mirroring Session

1 Open the **Port Mirroring** page.

2 Modify the fields.

3 Click **Apply Changes**.

The port mirroring session fields are modified, and the device is updated.

Deleting a Port Mirroring Session

1 Open the **Port Mirroring** page.

2 Check the **Remove** check box.

3 Click **Apply Changes**.

The port mirroring session is deleted, and the device is updated.

Configuring a Port Mirroring Session Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring a Port Mirroring session as displayed in the *Port Mirroring*.

Table 7-11. Port Mirroring CLI Commands

CLI Command	Description
`port monitor src-interface [rx | tx]`	Starts a port monitoring session.
`show ports monitor`	Displays status of port monitoring.

The following is an example of the CLI commands:

```
Console(config-if)# port monitor g2
```

Configuring Address Tables

MAC addresses are stored in either the static address or the dynamic address database. Static addresses are defined by the user. Dynamic addresses are learned by the system, and are erased after a time-out. A packet addressed to a destination stored in one of the databases is forwarded immediately to the ports. The static and dynamic address tables can be sorted by interface, VLAN, and interface type. In addition, addresses can be added to the static and dynamic address tables.

To open the **Address Tables** page, click **Switch→Address Table** in the tree view.

Defining Static Addresses

The **Static Address** page contains a list of static MAC addresses. A static address can be added and removed from the Static MAC Address Table. To open the **Static Address** page, click **Switch→ Address Table→Static Address** in the tree view.

Figure 7-17. Static MAC Address Page

Interface — The specific port or LAG to which the static MAC address is applied.

MAC Address — The MAC address listed in the current static address list.

NOTE: Only MAC addresses assigned to the specified interface and VLAN are displayed. To view MAC addresses assigned to a different VLAN, choose the VLAN from the VLAN selector.

VLAN ID — The VLAN ID attached to the MAC Address.

VLAN Name — User-defined VLAN name.

Status — Status of the MAC address. Possible values are:

Secure — Guarantees that a locked port MAC address is not deleted.

Permanent — The MAC address is permanent.

Delete on Reset — The MAC address is deleted when the device is reset.

Delete on Timeout — The MAC address is deleted when a timeout occurs.

Adding a Static MAC Address

1. Open the **Static MAC Address** page.
2. Click **Add** to display the **Add Static MAC Address** page.
3. Complete the fields.
4. Click **Apply Changes**.

   The new static address is added to the **Static MAC Address Table**, and the device is updated.

Modifying a Static Address in the Static MAC Address Table

1. Open the **Static MAC Address** page.
2. Modify the fields.
3. Click **Apply Changes**.

   The static MAC address is modified, and the device is updated.

Removing a Static Address from the Static Address Table

1. Open the **Static MAC Address** page.
2. Click **Show All** to display the **Static MAC Address Table**.
3. Select a table entry.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The static address is deleted, and the device is updated.

Configuring Static Address Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring static address parameters as displayed in the *Static MAC Address Page*.

Table 7-12. Static Address CLI Commands

CLI Command	Description
`bridge address mac-address {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`} [permanent | delete-on-reset | delete-on-timeout | secure]`	Adds a static MAC-layer station source address to the bridge table.

Table 7-12. Static Address CLI Commands

CLI Command	Description
`show bridge address-table static [vlan vlan] [ethernet interface | port-channel port-channel-number]`	Displays statically created entries in the bridge-forwarding database.

The following is an example of the CLI commands:

```
console (config)# interface vlan 1 console

(config-vlan)# bridge address 3aa2.64b3.a245 ethernet g8 permanent….


Console (config-vlan)# exit

Console (config)# exit

Console> show bridge address-table static


Aging time is 300 sec


 Vlan       Mac Address       Port         Type

------ -------------------- ------ ------------------

  1      3a:a2:64:b3:a2:45     g8        permanent
```

Viewing Dynamic Addresses

The **Dynamic Addresses Table** contains fields for querying information in the dynamic address table, including the interface type, MAC addresses, VLAN, and table sorting key. Packets forwarded to an address stored in the address table are forwarded directly to those ports.

The **Dynamic Address Table** also contains information about the aging time before a dynamic MAC address is removed from the table.

To open the **Dynamic Address Table**, click **Switch→Address Tables→Dynamic Addresses Table** in the tree view.

Figure 7-18. Dynamic Address Table

The **Dynamic Address Table** contains the following fields:

Address Aging (10-630) — Specifies aging time in seconds before a dynamic MAC address is erased. The default value is 300 seconds.

The Dynamic Address Table can be queried by:

Port — Interface queried for an address.

MAC Address — The MAC address queried for an address.

VLAN ID — The VLAN number (to which the MAC address is attached) that is queried for an address.

Address Table Sort Key — Specifies if the Dynamic Address Table is sorted by address, VLAN or interface.

Defining the Aging Time

1. Open the **Dynamic Address Table** page.
2. Define the **Address Aging** field.
3. Click **Apply Changes**.

   The aging time is modified, and the device is updated.

Querying the Dynamic Address Table

1. Open the **Dynamic Address Table** page.
2. Define the parameter by which to query the **Dynamic Address Table**.

Entries can be queried by **Port**, **MAC Address**, or **VLAN ID**.

3 Click **Query**.

The Dynamic Address Table is queried.

Sorting the Dynamic Address Table

1 Open the **Dynamic Address Table** page.

2 From the **Address Table Sort Key** drop-down menu, select whether to sort addresses by address, VLAN ID, or interface.

3 Click **Query**.

The Dynamic Address Table is sorted.

Current Address Table

The Current Address Table contains dynamic address parameters by which packets are directly forwarded to the ports. The Current Address Table contains the following fields:

- VLAN ID — Indicates the VLAN Tag value.
- MAC — Indicates the MAC address.
- Port — Indicates the port number.

Querying and Sorting Dynamic Addresses Using CLI Commands

The following table summarizes the equivalent CLI commands for querying and sorting dynamic addresses as displayed in the **Dynamic Address Table**.

Table 7-13. Query and Sort CLI Commands

CLI Command	Description
`bridge aging-time` *`seconds`*	Sets the address table aging time.
`show bridge address-table [vlan vlan] [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays classes of dynamically created entries in the bridge-forwarding database.

The following is an example of the CLI commands:

```
Console (config)# bridge aging-time 300

Console (config)# exit

Console# show bridge address-table

Aging time is 300 sec
```

```
vlan mac address port type
---- -------------- ----- -----
1 0060.704C.73FF g8 dynamic
1 0060.708C.73FF g8 dynamic
200 0010.0D48.37FF g9 static
```

Configuring GARP

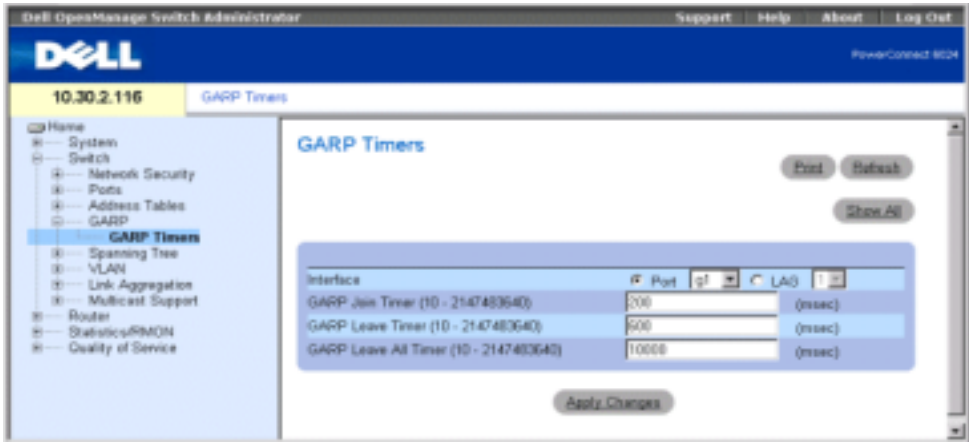
Generic Attribute Registration Protocol (GARP) is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address.

To open the **GARP** page, click **Switch→GARP** in the tree view.

Defining GARP Timers

The **GARP Timers** page contains parameters for enabling GARP on the device. To open the **GARP Timers** page, click **Switch→GARP →GARP Timers** in the tree view.

Figure 7-19. GARP Timers



The **GARP Timers** page contains the following fields:

Interface — Determines if enabled on a port or on a LAG.

GARP Join Timer (10 - 2147483640) — Time, in milliseconds, that PDUs are transmitted. The possible field value is 10-2147483640. The default value is 200 msec.

GARP Leave Timer (10 - 2147483640) — Time lapse, in milliseconds, that the device waits before leaving its GARP state. Leave time is activated by a Leave All Time message sent/received, and cancelled by the Join message received. Leave time must be greater than or equal to three times the join time. The possible field value is 0-2147483640. The default value is 600 msec.

GARP Leave All Timer (10 - 2147483640)—Time lapse, in milliseconds, that all devices wait before leaving the GARP state. The leave all time must be greater than the leave time. The possible field value is 0-2147483640. The default value is 10,000 msec.

Defining GARP Timers

1. Open the **GARP Timers** page.
2. Complete the fields.
3. Click **Apply Changes**.

   The GARP parameters are saved to the device.

Copying Parameters in the GARP Timers Table

1. Open the **GARP Timers** page.
2. Click **Show All** to display the **GARP Timers Table**.
3. Select the interface type in the **Copy Parameters from** field.
4. Select an interface in either the **Port** or **LAG** drop-down menu.
5. The definitions for this interface will be copied to the selected interfaces. See step 6.
6. Check the **Copy to** check box to define the interfaces to which the GARP timer definitions are copied, or click **Select All** to copy the definitions to all ports or LAGs.
7. Click **Apply Changes**.

   The parameters are copied to the selected port ports or LAGs in the GARP Timers Table, and the device is updated.

Defining GARP Timers Using CLI Commands

Table 7-14 summarizes the equivalent CLI commands for defining GARP timers as displayed in the **Garp Timers** page.

Table 7-14. GARP Timer CLI Commands

CLI Command	Description
`garp timer {join | leave | leaveall} timer_value`	Adjusts the GARP application join, leave, and leaveall GARP timer values.

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g8
Console (config-if)# garp timer leave 900
```

Configuring the Spanning Tree Protocol

The Spanning Tree Protocol (STP) provides a tree topology for any arrangement of bridges. STP also provides one path between end stations on a network, eliminating loops.

Loops occur when alternate routes exist between hosts. Loops in an extended network can cause bridges to forward traffic indefinitely, resulting in increased traffic and reduced network efficiency.

The device supports the following spanning tree versions: Classic STP, Rapid STP and Multiple STP.

Classic STP provides a single path between end station, avoiding and eliminating loops. For information on configuring Classic STP, see **Defining STP Global Settings**.

Rapid STP (RSTP) detects and uses network topologies that provide faster convergence of the spanning tree without creating forwarding loops. For information on configuring RSTP, see **Defining the Rapid Spanning Tree**.

Multiple STP (MSTP) provides full connectivity for packets allocated to any VLAN. MSTP is based on RSTP. In addition, MSTP transmits packets assigned to different VLANS through different MST regions. MST regions act as a single bridge. MSTP increases system fault tolerance and enables load balancing. For information on configuring MSTP, see **Defining the Multiple Spanning Tree**.

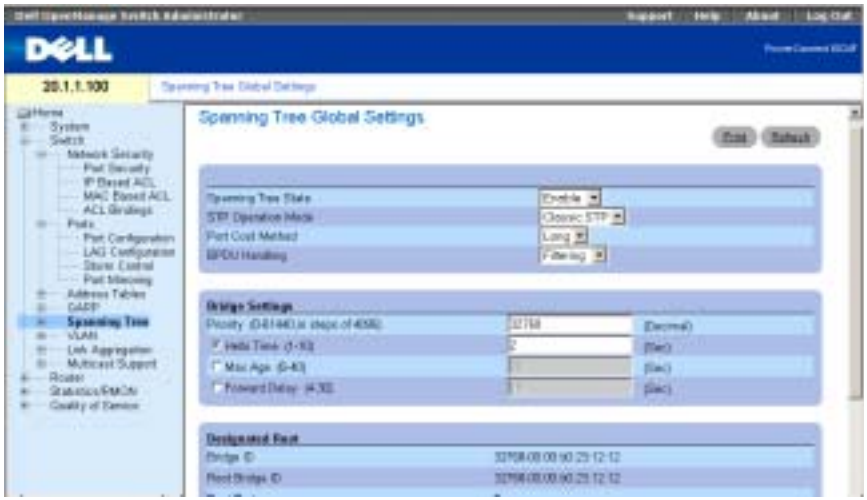
To open the **Spanning Tree** page, click **Switch→Spanning Tree** in the tree view.

Defining STP Global Settings

The **Spanning Tree Global Settings** page contains parameters for enabling STP on the device.

To open the **Spanning Tree Global Settings** page, click **Switch→Spanning Tree→Global Settings** in the tree view.

Figure 7-20. Spanning Tree Global Settings



The **Spanning Tree Global Settings** page contains the following fields:

Spanning Tree State — Enables or disables STP, RSTP or MSTP on the device.

STP Operation Mode — The STP mode by which STP is enabled on the device. Possible field values are: **Classic STP**, **Rapid STP, and Multiple STP**.

Path Cost Method — Specifies the method used to assign default path costs to STP ports. The possible field values are:

Long — Path cost method with a range of 1-200,000,000.

Short — Path cost method with a range of 1-65,535. This is the default method.

The default path costs assigned to an interface vary according to the selected method:

Interface	Long	Short
LAG	20,000	4
1000 Mbps	20,000	4
100 Mbps	200,000	19
10 Mbps	2,000,000	100

BPDU Handling — Specifies BPDU packet handling when the spanning tree is disabled on an interface. The possible field values are Filtering and Flooding. The default value is Flooding.

Priority (0-65535) — The bridge priority value. When switches or bridges are running STP, each are assigned a priority. After exchanging BPDUs, the switch with the lowest priority value becomes the root bridge. The default value is 32768.

Hello Time (1-10) — The switch Hello time, which indicates the amount of time in seconds a root bridge waits between configuration messages. The default value is 2.

Max Age (6-40) — The switch maximum age time, which indicates the amount of time in seconds a bridge waits before implementing a topological change. The default value is 20.

Forward Delay (4-30)— The switch forward delay time, which indicates the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. The default value is 15.

Bridge ID — The bridge ID.

Root Bridge ID — The root bridge ID.

Root Port — Port number that offers the lowest-cost path from this bridge to the root bridge. It is significant when the bridge is not the root. The default is zero.

Root Path Cost — Cost of the path from this bridge to the root.

Topology Changes Counts — Total amount of STP state changes that have occurred.

Last Topology Change — Total amount of time since the last topographic change. The time is displayed in hour/minute/second format, for example, 5 hours 10 minutes and 4 seconds.

Defining STP Global Parameters

1. Open the **Spanning Tree Global Settings** page.
2. Select the port that you want to enable from the **Select a Port** drop-down menu.
3. Select **Enable** in the **Spanning Tree State** field.
4. Select the **STP** mode in the **STP Operation Mode** field, and define the bridge settings.
5. Click **Apply Changes**.

   STP is enabled on the device.

Modifying STP Global Parameters:

1. Open the **Spanning Tree Global Settings** page.
2. Define the fields in the dialog.
3. Click **Apply Changes**.

   The STP parameters are modified, and the device is updated.

Defining STP Global Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP global parameters as displayed in the **Spanning Tree Global Settings** page.

Table 7-15. STP Global Settings CLI Commands

CLI Command	Description
`spanning-tree`	Enables spanning tree functionality.
`spanning-tree mode {stp | rstp}`	Configures the spanning tree protocol mode.
`spanning-tree pathcost method {long | short}`	Configures the spanning tree path cost method.
`spanning-tree bpdu {filtering | flooding}`	Configures handling BPDU packets when the spanning tree is disabled on an interface.
`spanning-tree priority` *priority*	Configures the spanning tree priority.
`spanning-tree hello-time` *seconds*	Configures the spanning tree bridge Hello Time, which is how often the switch broadcasts Hello messages to other switches.
`spanning-tree max-age` *seconds*	Configures the spanning tree bridge maximum age.
`spanning-tree forward-time` *seconds*	Configures the spanning tree bridge forward time, which is the amount of time a port remains in the listening and learning states before entering the forwarding state.
`show spanning-tree [ethernet` *interface* `| port-channel` *port-channel-number*`]`	Displays spanning tree configuration.

The following is an example of the CLI commands:

```
Console(config)# spanning-tree
Console(config)# spanning-tree mode rstp
Console(config)# spanning-tree priority 12288
Console(config)# spanning-tree hello-time 5
Console(config)# spanning-tree max-age 10
Console(config)# spanning-tree forward-time 25
Console(config)# exit
Console# show spanning-tree
```

```
Spanning tree enabled mode RSTP
Root ID Priority 32768
Address 0001.4297.e000
Cost 57
Port g1
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Bridge ID Priority 32769
Address 0002.4b29.7a00
Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec
Number of topology changes 8 last change occurred 00:37:24 ago
Times: hold 1, topology change 35, notification 2
hello 2, max age 20, forward delay 15
```

Interface Name	Port ID Prio	Sts	Enb	Cost	Designated Cost	Bridge Id		Port ID Prio.Nbr	
g1	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	001
g2	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	002
g3	128	DSBL	FALSE	100	0	8000	00:00:b0:70:09:00	80	003
ch1	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	019
ch2	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01a
ch3	128	DSBL	TRUE	4	0	8000	00:00:b0:70:09:00	80	01b

Defining STP Port Settings

Use the **STP Port Settings** page to assign STP properties to individual ports.

To open the **STP Port Settings** page, click **Switch→Spanning Tree→Port Settings** in the tree view.

Figure 7-21. STP Port Settings

The **STP Port Settings** page contains the following fields:

Select a Port — Port on which STP is enabled.

STP — Enables or disables STP on the port.

Fast Link — When checked, enables Fast Link mode for the port. If Fast Link mode is enabled for a port, the **Port State** is automatically placed in the **Forwarding** state when the port link is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

Port State—Indicates the current STP state of a port. If enabled, the port state determines what forwarding action is taken on traffic. Possible port states are:

Disabled — STP is currently disabled on the port. The port forwards traffic while learning MAC addresses.

Blocking — The port is currently blocked and cannot be used to forward traffic or learn MAC addresses.

Listening — The port is currently in the listening mode. The port cannot forward traffic nor can it learn MAC addresses.

Learning — The port is currently in the learning mode. The port cannot forward traffic, however, it can learn new MAC addresses.

Forwarding — The port is currently in the forwarding mode. The port can forward traffic and learn new MAC addresses.

Speed — Speed at which the port is operating.

Path Cost (1-200,000,000) — The port contribution to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path is being rerouted.

Default Path Cost — Indicates that the default path cost is assigned according to the method selected on the **Spanning Tree Global Settings** page.

Priority (0-240) — Priority value of the port. The priority value influences the port choice when a bridge has two ports connected in a loop.

Designated Bridge ID — The ID of the designated bridge.

Designated Port ID— The ID of the selected port.

Designated Cost — Cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

Forward Transitions — Number of times the port has changed from the **Forwarding** state to **Disabled**.

LAG — The LAG to which the port is attached.

Enabling STP on a Port

1. Open the **STP Port Settings** page.
2. Select **Enabled** in the **STP Port Status** field.
3. Define the **Fast Link**, **Path Cost**, and the **Priority** fields.
4. Click **Apply Changes**.

   STP is enabled on the port.

Modifying STP Port Properties

1. Open the **STP Port Settings** page.
2. Modify the **Priority**, **Fast Link**, **Path Cost**, and the **Fast Link** fields.
3. Click **Apply Changes**.

   The STP port parameters are modified, and the device is updated.

Displaying the STP Port Table

1. Open the **STP Port Settings** page.
2. Click **Show All**.

   The **STP Port Table** opens.

Defining STP Port Settings Using CLI Commands

The following table summarizes the equivalent CLI commands for defining STP port parameters as displayed in the **STP Port Settings** page.

Table 7-16. STP Port Settings CLI Commands

CLI Command	Description
`spanning-tree disable`	Disables spanning tree on a specific port.
`spanning-tree cost` *`cost`*	Configures the spanning tree path cost for a port.
`spanning-tree port-priority` *`priority`*	Configures port priority.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Displays spanning tree configuration.
`spanning-tree portfast`	Enables PortFast mode.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree disable
Console(config-if)# spanning-tree cost 35000
Console(config-if)# spanning-tree port-priority 96
Console(config-if)# spanning-tree portfast
Console(config-if)# exit
Console(config)# exit
Console# show spanning-tree ethernet g1
Interface  Port ID  Designated                          Port ID
Name       Prio.Nbr Cost  Sts  Cost Bridge ID           Prio.Nbr
--------   -------  ---   --   --------------------     ------
g1         128.1    19    FWD  38 32768 0030.9441.62c1  128.25
Spanning tree enabled
Type: point-to-point (configured
: auto)
```

```
Port Fast: no (configured: no)
```

Defining STP LAG Settings

Use the **STP LAG Settings** page to assign STP aggregating ports parameters. To open the **STP LAG Settings** page, click **Switch→Spanning Tree→LAG Settings** in the tree view.

Figure 7-22. STP LAG Settings

The **STP LAG Settings** page contains the following fields:

Select a LAG — The LAG number for which you want to modify STP settings.

STP — Enables or disables STP on the LAG.

Fast Link — Enables Fast Link mode for the LAG. If Fast Link mode is enabled for a LAG, the **LAG State** is automatically placed in the **Forwarding** state when the LAG is up. Fast Link mode optimizes the time it takes for the STP protocol to converge. STP convergence can take 30-60 seconds in large networks.

LAG State — Current STP state of a LAG. If enabled, the LAG state determines what forwarding action is taken on traffic. If the bridge discovers a malfunctioning LAG, the LAG is placed in the **Broken** state. Possible LAG states are:

Disabled — STP is currently disabled on the LAG. The LAG forwards traffic while learning MAC addresses.

Blocking — The LAG is blocked and cannot be used to forward traffic or learn MAC addresses.

Listening — The LAG is in the listening mode and cannot forward traffic or learn MAC addresses.

Learning — The LAG is in the learning mode and cannot forward traffic, but it can learn new MAC addresses.

Forwarding — The LAG is currently in the forwarding mode, and it can forward traffic and learn new MAC addresses.

Broken — The LAG is currently malfunctioning and cannot be used for forwarding traffic.

Path Cost (1-200000000) — Amount the LAG contributes to the root path cost. The path cost is adjusted to a higher or lower value, and is used to forward traffic when a path being rerouted.

Default Path Cost — Indicates that the default path cost is assigned according to the method selected on the **Spanning Tree Global Settings** page.

Priority (0-240) — Priority value of the LAG. The priority value influences the LAG choice when a bridge has two looped ports. The priority value is between 0-240, in steps of 16.

Designated Bridge ID — Designated bridge ID.

Designated Port ID— Designated port ID.

Designated Cost — Cost of the port participating in the STP topology. Ports with a lower cost are less likely to be blocked if STP detects loops.

Forward Transitions — Number of times the **LAG State** has changed from the **Forwarding** state to **Disabled**.

Modifying the LAG STP Parameters

1. Open the **STP LAG Settings** page.
2. Select a LAG from the **Select a LAG** drop-down menu.
3. Modify the fields as desired.
4. Click **Apply Changes**.

   The STP LAG parameters are modified, and the device is updated.

Defining STP LAG Settings Using CLI Commands

The following table contains the CLI commands for defining STP LAG settings.

Table 7-17. STP LAG Settings CLI Commands

CLI Command	Description
`spanning-tree`	Enables spanning tree.

Table 7-17. STP LAG Settings CLI Commands

CLI Command	Description
`spanning-tree cost` *`cost`*	Configures the spanning tree path cost for a port.
`spanning-tree port-priority` *`priority`*	Configures port priority.
`show spanning-tree [ethernet interface | port-channel` *`port-channel-number`*`]`	Displays spanning tree configuration.
`spanning-tree portfast`	Enables Port Fast mode.

The following is an example of the CLI commands:

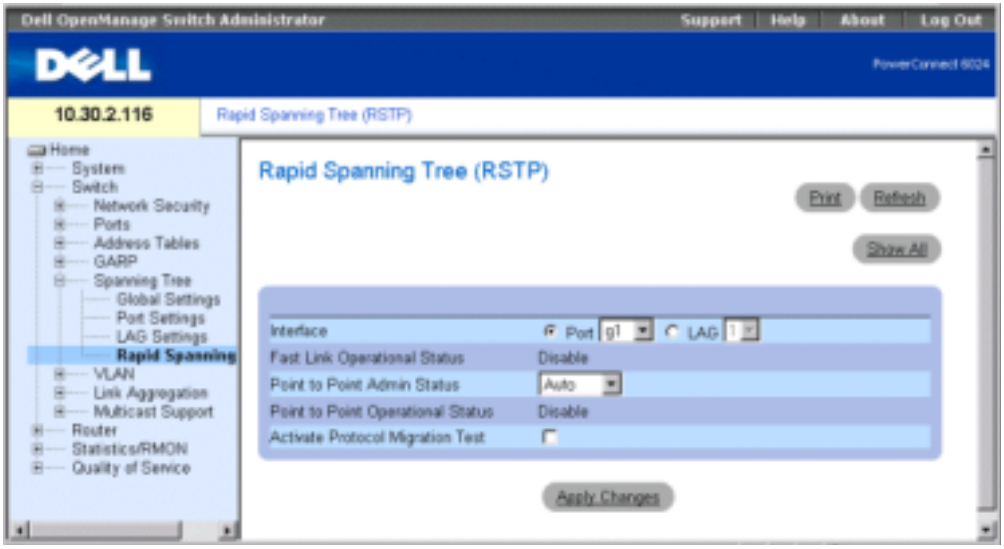
```
Console(config)# interface port-channel 1

Console(config-if)# spanning-tree disable

Console(config-if)# spanning-tree cost 35000

Console(config-if)# spanning-tree port-priority 96

Console(config-if)# spanning-tree portfast

Console(config-if)# exit

Console(config)# exit

Console# show spanning-tree port-channel 1

Interface Port ID                  Designated
Port ID

Name  Prio  Sts    Enb    Cost Cost Bridge Id        Prio.Nbr

------ ---- ------ ----- -------- --------- ---------------------
ch1    96   DSBL  FALSE   35000    0   32768 00:00:b0:11:00:00  96 25


Spanning tree disabled

Port Fast: yes (configured: yes)

Type: point-to-point (configured: auto)

Number of transitions to forwarding state: 0
```

Defining the Rapid Spanning Tree

While the classic spanning tree prevents Layer 2 forwarding loops on a general network topology, convergence can take 30-60 seconds. The delay allows time to detect possible loops, and propagate status changes.

Rapid Spanning Tree Protocol (RSTP) detects and uses network topologies that allow a faster convergence of the spanning tree, without creating forwarding loops. To open the **Rapid Spanning Tree (RSTP)** page, click **Switch→Spanning Tree→Rapid Spanning Tree** in the tree view.

Figure 7-23. Rapid Spanning Tree (RSTP) Page



Interface — Port or LAG on which Rapid STP is enabled.

Fast Link Operational Status — Indicates if Fast Link is enabled or disabled for the port or LAG. If Fast Link is enabled for a port, the port is automatically placed in the forwarding state.

Point-to-Point Admin Status — Enables or disables the device to establish a point-to-point link, or specifies for the device to automatically establish a point-to-point link.

To establish communications over a point-to-point link, the originating PPP first sends Link Control Protocol (LCP) packets to configure and test the data link. After a link is established and optional facilities are negotiated as needed by the LCP, the originating PPP sends Network Control Protocols (NCP) packets to select and configure one or more network layer protocols. When each of the chosen network layer protocols has been configured, packets from each network layer protocol can be sent over the link. The link will remain configured for communications until explicit LCP or NCP packets close the link, or until some external event occurs. This is the actual switch port link type. It may differ from the administrative state.

Point-to-Point Operational Status — The Point-to-Point operating state.

Activate Protocol Migration Test — When checked, enables PPP sending Link Control Protocol (LCP) packets to configure and test the data link.

Enabling RSTP

1. Open the **Rapid Spanning Tree (RSTP)** page.
2. Define the **Point-to-Point Admin**, **Point-to-Point Oper**, and the **Activate Protocol Migration** fields.
3. Click **Apply Changes**.

   The Rapid STP is enabled, and the device is updated.

Displaying the Rapid Spanning Tree (RSTP) Table

1. Open the **Rapid Spanning Tree (RSTP)** page.
2. Click **Show All**.

   The **Rapid Spanning Tree (RSTP) Table** opens.

Defining Rapid STP Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for defining Rapid STP parameters as displayed in the **RSTP** page.

Table 7-18. RSTP Settings CLI Command

CLI Command	Description
`spanning-tree link-type {point-to-point | shared}`	Overrides the default link-type setting.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g5
Console(config-if)# spanning-tree link-type shared
```

Defining the Multiple Spanning Tree

The Multiple Spanning Tree Protocol (MSTP) operation maps VLANs into STP instances.

MSTP provides a differing load balancing scenario. For example, while port A is blocked in one STP instance, the same port is placed in the Forwarding State in another STP instance. The **MSTP Settings** page allows defining up to sixteen MSTP instances for the device.

In addition, packets assigned to various VLANs are transmitted along different paths within Multiple Spanning Trees Regions (MST regions). Regions are one or more interconnected Multiple Spanning Tree bridges with identical MSTP configuration. In configuring an MST, the MST region to which your device belongs is defined. A configuration consists of the name, revision and region to which your device belongs.

To open the **MSTP Settings** page, click **Switch →Spanning Tree →MSTP Region Configuration** in the tree view.

Figure 7-24. MSTP Settings

The **MSTP Settings** page contains the following fields divided into two sections:

Region Name (1-32) — Specifies a user-defined MST region name.

Revision (0-65535) — Specifies unsigned 16-bit number that identifies the revision of the current MST configuration. The revision number is required as part of the MST configuration.

Max Hops (1-40) — Specifies the total number of hops that occur in a specific region before the BPDU is discarded. Once the BPDU is discarded, the port information is aged out. The default field value is 20.

IST Master — Indicates the Internal Spanning Tree Master ID. The IST Master is the root of the specified instance and its instance is 0.

Instance ID — Specifies the ID of the spanning tree instance. The field range is 1-15.

Included VLANs— Maps the selected VLANs to the selected instance. Every VLAN belongs to one instance only.

Bridge Priority (0-61440) — Specifies the device priority for the selected spanning tree instance.

Designated Root Bridge ID — Indicates the ID of the bridge with the lowest path cost to the instance root.

Root Port — Indicates the root port of the selected instance.

Root Path Cost — Indicates the path cost of the selected instance to the region root.

Bridge ID — Indicates the bridge ID of the selected instance.

Remaining Hops — Indicates the number of hops remaining to the next destination.

Displaying the MSTP VLAN to Instance Mapping Table

1. Open the **MSTP Settings** page.
2. Click **Show All**.

   The **MSTP VLAN to Instance Mapping Table** page opens:

Figure 7-25. MSTP VLAN to Instance Mapping Table

Defining MST Instances Using CLI Commands

The following table summarizes the equivalent CLI commands for defining MST instance groups as displayed in the **MSTP Settings** page.

Table 7-19. MSTP Instances CLI Commands

CLI Command	Description
`spanning-tree mst configuration`	Enters the MST Configuration mode.
`instance` *`instance-id`* `{add | remove} vlan` *`vlan-range`*	Maps VLANs to the MST instance.
`name` *`string`*	Sets the configuration name.
`revision` *`value`*	Sets the configuration revision number
`spanning-tree mst` *`instance-id`* `port-priority` *`priority`*	Sets the port priority.

Table 7-19. MSTP Instances CLI Commands

CLI Command	Description
`spanning-tree mst` *`instance-id`* `priority` *`priority`*	Sets the device priority for the specified spanning tree instance.
`spanning-tree mst max-hops` *`hop-count`*	Sets the number of hops in an MST region before the BPDU is discarded and the information held for a port is aged.
`spanning-tree mst` *`instance-id`* `cost` *`cost`*	Sets the path cost of the port for MST calculations
`exit`	Exits the MST Configuration mode and applies configuration changes.
`abort`	Exits the MST Configuration mode without applying configuration changes.
`show {current | pending}`	Displays the current or pending MST region configuration.

The following is an example of the CLI commands:

```
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 1 add vlan 10-20
Console(config-mst)# name region1
Console(config-mst)# revision 1
Console(config)# spanning-tree mst configuration
Console(config-mst)# instance 2 add vlan 21-30
Console(config-mst)# name region1
Console(config-mst)# revision 1
Console(config-mst)# show pending
Pending MST configuration
```

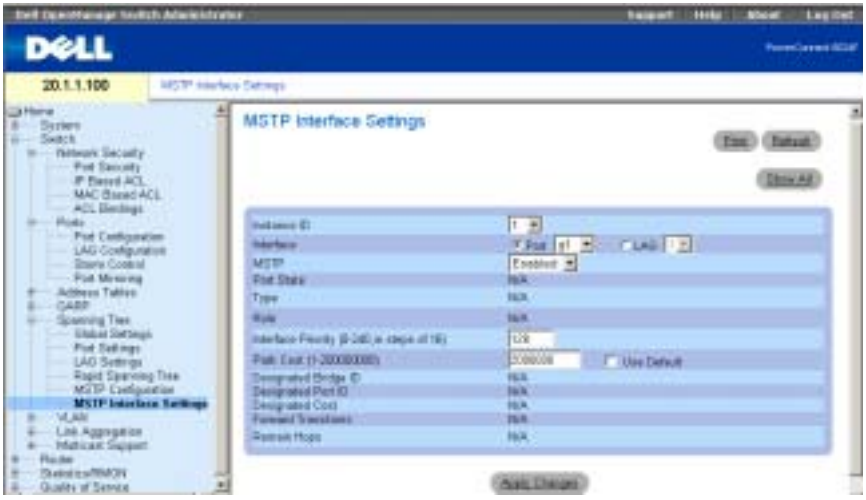
```
Name: Region1
Revision: 1
Instance        Vlans Mapped
--------        ------------
0               1-9,31-4094
1               10-20
2               21-30
```

Defining MSTP Interface Settings

Use the **MSTP Interface Setting** page to assign MSTP settings to specific interfaces.

To open the **MSTP Interface Setting** page, click **Switch →Spanning Tree →MSTP Interface Setting** in the tree view.

Figure 7-26. MSTP Interface Setting



The **MSTP Interface Setting** page contains the following parameters:

Instance ID — Lists the MSTP instances configured on the device. Possible field range is 0-15.

Interface — Assigns either ports or LAGs to the selected MSTP instance.

Port State— Indicates whether the port is enabled or disabled in the specific instance.

Type — Indicates whether MSTP treats the port as a point-to-point port or a port connected to a hub and whether the port is internal to the MST region or a boundary port. If the port is a boundary port, it also indicates whether the device on the other side of the link is working in RSTP or STP mode

Role — Indicates the port role assigned by the STP algorithm in order to provide to STP paths. The possible field values are:

Root — Provides the lowest cost path to forward packets to root device.

Designated — Indicates the port or LAG via which the designated device is attached to the LAN.

Alternate — Provides an alternate path to the root device from the interface.

Backup — Provides a backup path to the designated LAN. Backup ports occur only when two ports are connected in a loop by a point-to-point link. Backup ports also occur when a LAN has two or more connections connected to a shared segment.

Disabled — Indicates the port is not participating in the Spanning Tree.

Interface Priority — Defines the interface priority for the specified instance. The priority range is 0-240 in steps of 16. The default value is 128.

Path Cost — Indicates the port contribution to the Spanning Tree instance. The range should always be 1-200,000,000.

Default Path Cost — Indicates that the default path cost is assigned according to the method selected on the **Spanning Tree Global Settings** page.

Designated Bridge ID — The bridge ID number that connects the link or shared LAN to the root.

Designated Port ID — The port ID number on the designated bridge that connects the link or the shared LAN to the root.

Designated Cost — Cost of the path from the link or the shared LAN to the root.

Forward Transitions — Number of times the port changed to the forwarding state.

Remain Hops — Indicates the number of hops remaining to the next destination.

Viewing the MSTP Interface Table

1. Open the **MSTP Interface Setting** page.
2. Click **Show All**.

   The **MSTP Interface Table** page opens:

Figure 7-27. MSTP Interface Table

Defining MSTP Interfaces Using CLI Commands

The following table summarizes the equivalent CLI commands for defining MSTP interfaces as displayed in the **MSTP Interface Setting** page.

Table 7-20. MSTP Interface CLI Commands

CLI Command	Description
`spanning-tree mst` *`instance-id`* `cost` *`cost`*	Sets the path cost of the port for MST calculations
`spanning-tree mst` *`instance-id`* `priority` *`priority`*	Sets the device priority for the specified ST instance.
`show spanning-tree mst-configuration`	Displays the MST configuration.

The following is an example of the CLI commands:

```
Console (config) # interface ethernet g9
Console (config-if) # spanning-tree mst 1 cost 4
Console (config-if)# spanning-tree mst 1 port-priority 142
Console (config-if)# end
Console# show spanning-tree
Spanning tree enabled mode MSTP
Default port cost method: long
###### MST 0 Vlans Mapped: 1-9, 21-4094
CST Root ID   Priority 32768
Address 00:01:42:97:e0:00
Path Cost     20000
```

```
Root Port    1 (ig)
Hello Time 2 sec       Max Age 20 sec  Forward Delay 15 sec
IST Master ID Priority     32768
Address            00:02:4b:19:7a:00
Path Cost    10000
Rem hops   19
Bridge ID Priority     32768
Address            00:02:4b:29:7a:00
Hello Time 2 sec     Max Age 20 sec  Forward Delay 15 sec
Max hops 20
```

Configuring VLANs

VLANs are logical subgroups with a LAN created via software, rather than defining a hardware solution. VLANs combine user stations and network devices into a single unit regardless of the physical LAN segment to which they are attached. VLANs allow network traffic to flow more efficiently within subgroups. VLANs managed through software reduce the amount of time network changes, additions, and moves are implemented.

VLANs have no minimum number of ports, and can be created per unit, per device, per stack, or any other logical connection combination, as VLANs are software based and not defined by physical attributes.

VLANs function at a layer 2 level. Since VLANs isolate traffic within the VLAN, a layer 3 router working a protocol level is needed to allows traffic flow between VLANs. Layer 3 routers identify segments and coordinate with VLANs. VLANs are broadcast and multicast domain. Broadcast and multicast traffic is transmitted only in the VLAN in which the traffic is generated.

VLAN tagging provides a method of transferring VLAN information between VLAN groups. VLAN tagging attaches a 4-byte tag to packet headers. The VLAN tag indicates to which VLAN the packet belongs. VLAN tags are attached to the VLAN by either the end station or by the network device. VLAN tags also contains VLAN network priority information.

Combining VLANs and GVRP allows network managers to define network nodes into broadcast domains. Broadcast and Multicast traffic is confined to the originating group.

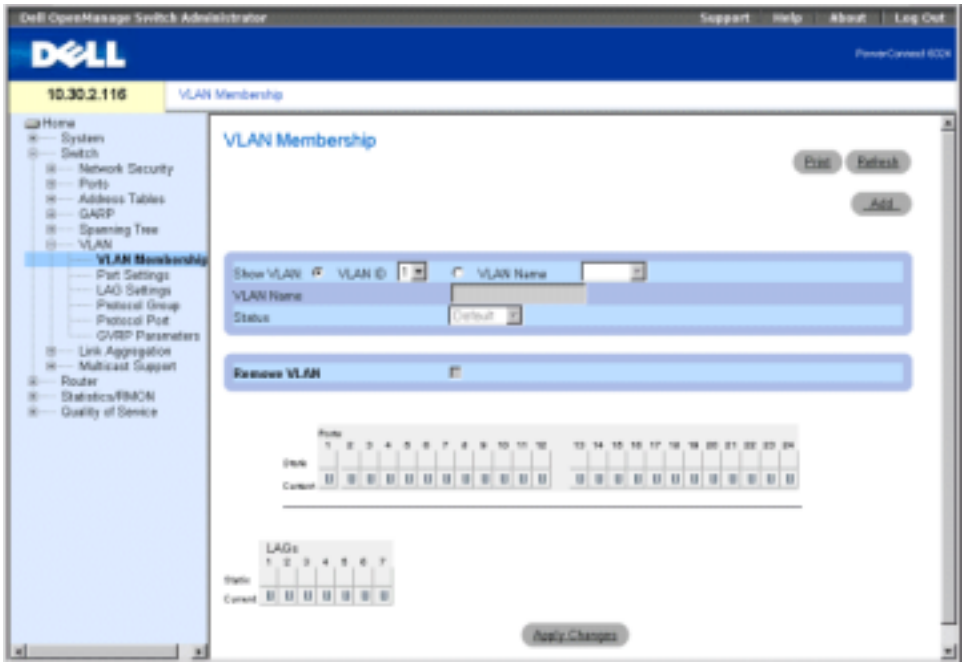
To display the **VLAN** page, click **Switch→VLAN** in the tree view.

Defining VLAN Membership

Use the **VLAN Membership** page to define VLAN groups.

To open the **VLAN Membership** page, click **Switch→VLAN→VLAN Membership** in the tree view.

Figure 7-28. VLAN Membership Page



The **VLAN Membership** page is divided into the VLAN Membership Table and the VLAN Port Membership Table.

VLAN Membership Table

The **VLAN Membership Table** contains parameters for assigning VLAN membership to ports. Your switch supports up to 4095 VLANs. However, you can actually create only 4062 VLANs because:

- VLANs 4064 through 4094 are reserved by the device for the internal operational usage,
- VLAN 1 is the default VLAN of which all ports are members by default, and
- VLAN 4095 is designated as the "Discard VLAN."

Show VLAN — Lists and displays specific VLAN information according to VLAN ID or VLAN name.

VLAN Name — Indicates the user-defined VLAN name.

Status—Indicates the VLAN type. Possible values are:

Dynamic — Indicates the VLAN was dynamically created through GVRP.

Static — Indicates the VLAN is user-defined.

Remove VLAN — When checked, removes the VLAN from the VLAN Membership Table.

Adding New VLANs

1. Open the **VLAN Membership** page.
2. Click **Add** to display the **Create New VLAN** page.
3. Enter the VLAN ID and name.
4. Click **Apply Changes**.

   The new VLAN is added, and the device is updated.

Modifying VLAN Membership Groups

1. Open the **VLAN Membership** page.
2. Select a VLAN from the **Show VLAN** drop-down menu.
3. Modify the fields as desired.
4. Click **Apply Changes**.

   The VLAN membership information is modified, and the device is updated.

Deleting VLAN Membership Groups

1. Open the **VLAN Membership** page.
2. Select a VLAN in the **Show VLAN** field.
3. Check the **Remove VLAN** check box.
4. Click **Apply Changes**.

   The VLAN is deleted, and the device is updated.

Defining VLAN Membership Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for defining VLAN membership groups as displayed in the **VLAN Membership** page.

Table 7-21. VLAN Membership Group CLI Commands

CLI Command	Description
`vlan database`	Enters the interface configuration (VLAN) mode.
`vlan {`*`vlan-range`*`}`	Creates a VLAN.
`name` *`string`*	Adds a name to a VLAN.

The following is an example of the CLI commands:

```
console (config)#interface vlan 1972
console (config-if)#name Marketing
```

VLAN Port Membership Table

The **VLAN Port Membership Table** contains a **Port Table** for assigning ports to VLANs. Ports are assigned VLAN membership by toggling through the **Port Control** settings. Ports can have the following values:

Table 7-22. VLAN Port Membership Table

Port Control	Definition
T	The interface Is a member of a VLAN. All packets forwarded by the interface are tagged. The packets contain VLAN information.
U	The interface is a VLAN member. Packets forwarded by the interface are untagged.
F	The interface is denied membership to a VLAN.
Blank	The interface is not a VLAN member. Packets associated with the interface are not forwarded.

The **VLAN Port Membership Table** displays the ports and the ports states, as well as LAGs.

Assigning Ports to a VLAN Group

1. Open **VLAN Membership** page.
2. Click the **VLAN ID** or **VLAN Name** option button and select a VLAN from the drop-down menu.
3. Select a port in the **Port Membership Table**, and assign the port a value.
4. Click **Apply Changes**.

   The port is assigned to the VLAN group, and the device is updated.

Deleting a VLAN

1. Open the **VLAN Membership** page.
2. Click the **VLAN ID** or **VLAN Name** option button and select a VLAN from the drop-down menu.
3. Check the **Remove VLAN** check box.
4. Click **Apply Changes**.

   The VLAN is deleted, and the device is updated.

Assigning Ports to VLAN Groups Using CLI Commands

The following table contains the CLI commands for assigning ports to VLAN groups.

Table 7-23. Port-to-VLAN Group Assignments CLI Commands

CLI Command	Description
`switchport general acceptable-frame-types tagged-only`	Discards untagged frames at ingress.
`switchport forbidden vlan {add` *`vlan-list`* `| remove` *`vlan-list`*`}`	Forbids adding specific VLANs to the port.

Examples of CLI command are as follows:

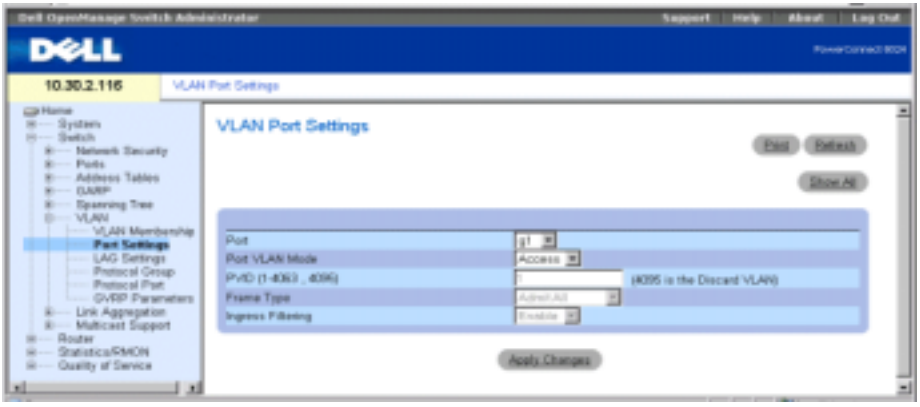
```
Console (config)# interface ethernet g1

Console(config-if)#switchport general acceptable-frame-types
tagged-only

Console (config-if)#switchport forbidden vlan add 234-256
```

Defining VLAN Port Settings

Use the **VLAN Port Settings** to provide parameters for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the **VLAN Port Settings** page. All untagged packets arriving to the device are tagged by the ports PVID.

To open the **VLAN Port Settings** page, click **Switch→VLAN→Port Settings** in the tree view.

Figure 7-29. VLAN Port Settings Page



Port — The port number included in the VLAN.

Port VLAN Mode — Indicates the port mode. Possible values are:

General — The port belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).

Access — The port belongs to a single untagged VLAN. When a port is in Access mode, the packet types which are accepted on the port (packet type) cannot be designated. It is also not possible to enable/disable ingress filtering on an access port.

Trunk — The port belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

PVID (1-4063, 4095)— Assigns a VLAN ID to untagged packets. The possible values are 1-4063 and 4095. VLAN 4095 is defined as per standard and industry practice as the discard VLAN; packets classified to this VLAN are dropped.

Frame Type — Frame type accepted on the port. Possible values are:

Admit Tag Only—Indicates that only tagged frames are accepted on the port.

Admit All—Indicates that both tagged and untagged frames are accepted on the port.

Ingress Filtering — Enables or disables Ingress filtering on the port. Ingress filtering discards frames where the VLAN tag does not match any port VLAN.

Assigning Port Settings

1. Open the **VLAN Port Settings** page.
2. Select the port to which you want to assign settings from the **Port** drop-down menu.
3. Complete the remaining fields on the page and click **Apply Changes**.

   The VLAN port settings are defined, and the device is updated.

Displaying the VLAN Port Table

1. Open the **VLAN Port Settings** page.
2. Click **Show All** to display the **VLAN Port Table**.

NOTE: If an **Access** port is chosen, the packet types that are accepted on the port (packet type) cannot be designated. It is also not possible to enable or disable ingress filtering on an access port.

Assigning Ports to VLAN Groups Using CLI Commands

The following table contains the CLI commands for assigning ports to VLAN groups.

Table 7-24. VLAN Port CLI Commands

CLI Command	Description
`switchport mode { access | trunk | general}`	Configures a port VLAN membership mode.
`switchport trunk native vlan` *`vlan-id`*	Defines the port as a member of the specified VLAN, and the VLAN ID as the "port default VLAN ID (PVID)".
`switchport general pvid` *`vlan-id`*	Configure the Port VLAN ID (PVID) when the interface is in general mode.
`switchport general allowed vlan add` *`vlan-list`* `[ tagged | untagged]`	Adds or removes VLANs from a general port.
`switchport general acceptable-packet-types tagged-only`	Discards untagged packets at ingress.
`switchport general ingress-filtering disable`	Disables port ingress filtering.
`shutdown`	Disables interfaces.
`set interface active {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Reactivates an interface that is shutdown due to security reasons.

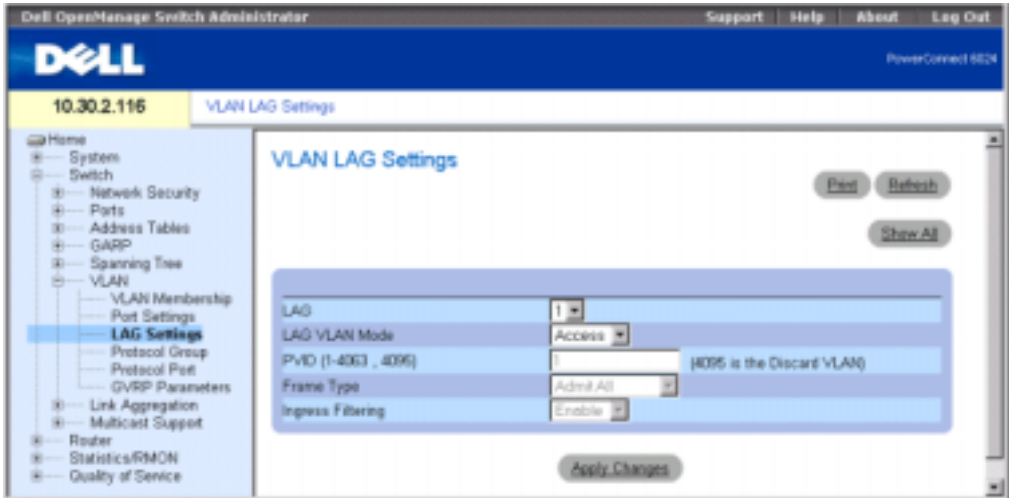
The following is an example of the CLI commands:

```
Console (config)# interface ethernet g8

Console (config-if)# switchport mode access

console (config-if)# switchport trunk native vlan 123

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6
tagged

Console (config-if)# switchport general acceptable-packet-types
tagged-only
```

Defining VLAN LAG Settings

The **VLAN LAG Settings** page provides parameters for managing LAGs that are part of a VLAN. VLANs can either be composed of individual ports or of LAGs. Untagged packets entering the switch are tagged with the LAGs ID specified by the PVID. To open the **VLAN LAG Settings** page, click **Switch→VLAN→LAG Settings** in the tree view.

Figure 7-30. VLAN LAG Setting Page



LAG — The LAG number included in the VLAN.

LAG VLAN Mode — Indicates the VLAN LAG mode. Possible values are:

General — The LAG belongs to VLANs, and each VLAN is user-defined as tagged or untagged (full 802.1Q mode).

Access — The LAG belongs to a single, untagged VLAN.

Trunk — The LAG belongs to VLANs in which all ports are tagged (except for an optional single native VLAN).

PVID (1-4063, 4095)— Assigns a VLAN ID to untagged packets. The possible field values are 1-4063 and 4095. VLAN 4095 is defined as per standard and industry practice as the discard VLAN; packets classified to this VLAN are dropped.

Frame Type — Packet type accepted by the LAG. Possible values are:

Admit Tag Only — Only tagged packets are accepted by the LAG.

Admit All — Tagged and untagged packets are both accepted by the LAG.

Ingress Filtering — Enables or disables Ingress filtering by the LAG. Ingress filtering discards packets where the VLAN tag does not match any LAG VLAN.

Assigning VLAG Settings

1. Open the **VLAN LAG Settings** page.
2. Select a LAG from the **LAG** drop-down menu and complete the fields on the page.
3. Click **Apply Changes**.

   The VLAN LAG parameters are defined, and the device is updated.

Displaying the VLAN LAG Table

1. Open the **VLAN LAG Settings** page.
2. Click **Show All** to display the **VLAN LAG Table**.

Assigning LAGs to VLAN Groups Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning LAGs to VLAN groups as displayed in the **VLAN LAG Settings** page.

Table 7-25. LAG VLAN Assignments CLI Commands

CLI Command	Description
`switchport mode {access | trunk | general}`	Configures a port VLAN membership mode.
`switchport trunk native vlan` *`vlan-id`*	Defines the port as a member of the specified VLAN, and the VLAN ID as the port default VLAN ID (PVID).
`switchport general pvid` *`vlan-id`*	Configure the Port VLAN ID (PVID) when the interface is in general mode.
`switchport general allowed vlan add` *`vlan-list`* `[tagged | untagged]`	Adds or removes VLANs from a general port.
`switchport general acceptable-frame-type tagged-only`	Discards untagged packets at ingress.
`switchport general ingress-filtering disable`	Disables port ingress filtering.

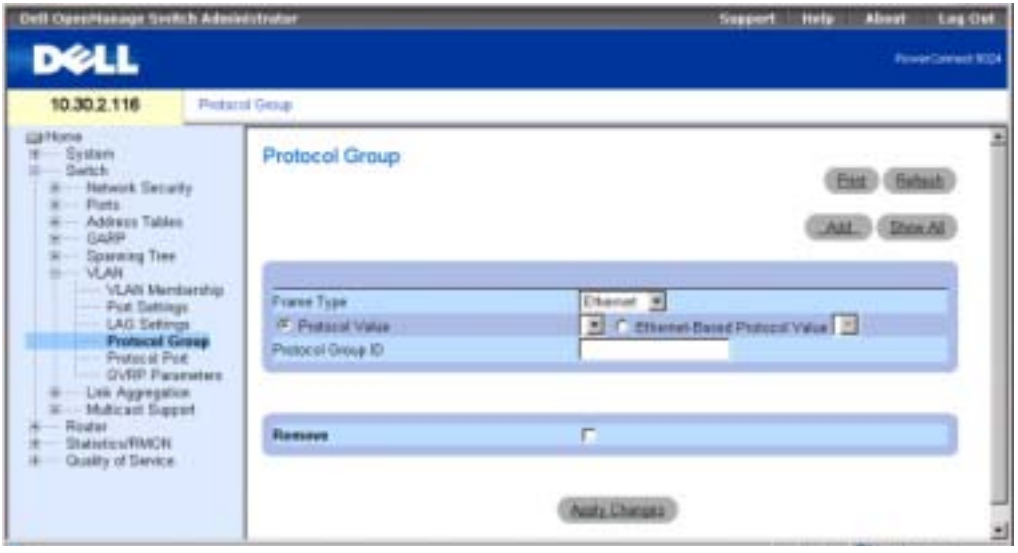
The following is an example of the CLI commands:

```
Console (config-if)# switchport mode access

Console (config-if)# switchport trunk native vlan 123

Console (config-if)# switchport general pvid 234

Console (config-if)# switchport general allowed vlan add 1,2,5,6
tagged

Console (config-if)# switchport general acceptable-frame-type
tagged-only
```

Defining VLAN Protocol Groups

The **Protocol Group** page contains information regarding protocol names and the VLAN Ethernet type. Interfaces can be classified as a specific protocol based interface. The classification places the interface into a protocol group.To open the **Protocol Group** page, click **Switch→VLAN→Protocol Group** in the tree view.

Figure 7-31. Protocol Group Table



Frame Type — The packet type. Possible field values are **Ethernet**, **RFC1042**, and **LLC Other**.

Protocol Value — User-defined protocol name.

Ethernet-Based Protocol Value — The Ethernet protocol group type.

Protocol Group ID — The VLAN Group ID number.

Adding a Protocol Group

1. Open the **Protocol Group** page.
2. Click **Add** to display the **Assign Protocol to Group** page.
3. Complete the fields on the page and click **Apply Changes**.

   The protocol group is assigned, and the device is updated.

Assigning VLAN Protocol Group Settings

1. Open the **Protocol Group** page.
2. Complete the fields on the page and click **Apply Changes**.

   The VLAN protocol group parameters are defined, and the device is updated.

Removing Protocols From the Protocol Group Table

1. Open the **Protocol Group** page.
2. Click **Show All** to display the **Protocol Group Table**.
3. Check **Remove** for the protocol groups that you want to remove.
4. Click **Apply Changes**.

   The protocol is removed, and the device is updated.

Defining VLAN Protocol Groups Using CLI Commands

The following table contains the CLI commands for configuring Protocol Groups.

Table 7-26. VLAN Protocol Groups CLI Commands

CLI Command	Description
`map protocol` *`protocol`* `[`*`encapsulation`*`] protocols-group` *`group`*	Adds a special protocol to a named group of protocols, which may be used for protocol-based VLAN assignment.

The following example maps ip-arp protocol to group "213":

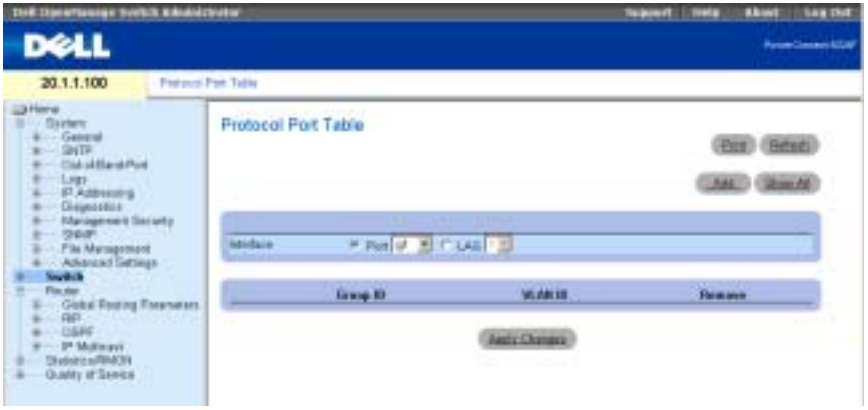
```
Console (config)# vlan database
Console (config-vlan)# map protocol ip-arp protocols-group 213
```

Adding Protocol Ports

The **Protocol Port** page adds interfaces to protocol groups.

To open the **Protocol Port** page, click **Switch→VLAN→Protocol Port** in the tree view.

Figure 7-32. Protocol Port Page



Interface — Port or LAG number added to a protocol group.

Protocol Group ID — Protocol group ID to which the interface is added. Protocol group IDs are defined in the Protocol Group Table.

VLAN ID — Attaches the interface to a user-defined VLAN ID. The VLAN ID is defined on the **Create a New VLAN** page. Protocol ports can either be attached to a VLAN ID or a VLAN name.

VLAN Name — Attaches the interface to a user-defined VLAN name. The VLAN name is defined on the **Create a New VLAN** page. This field is available only on the **Add Protocol Port** page.

Remove — When checked, removes the port assignment from a VLAN or protocol group.

Adding a New Protocol Port

1. Open the **Protocol Port Table** page.
2. Click **Add** to display the **Add Protocol Port** page.
3. Complete the fields in the dialog and click **Apply Changes**.

   The new VLAN protocol group is added to the **Protocol Port Table**, and the device is updated.

Defining Protocol Ports Using CLI Commands

The following table contains the CLI commands for defining Protocol Ports.

Table 7-27. Protocol Port CLI Commands

CLI Command	Description
`switchport general map protocols-group` *`group`* `vlan` *`vlan-id`*	Sets a protocol-based classification rule.

The following example sets a protocol-based classification rule of protocol group 1 to VLAN 8:

```
Console (config-if)# switchport general map protocols-group 1 vlan
8
```

Configuring GVRP

GARP VLAN Registration Protocol (GVRP) is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge and register VLAN membership.

To minimize the memory requirements when running the GVRP protocol, two proprietary tuning variables have been added to the standard variables:

- **Maximum number of GVRP VLANs** — Number of GVRP VLANs allowed to participate in GVRP operation.
- **Maximum number of GVRP VLANs after Reset** — Maximum number of GVRP VLANs after Reset is used for tuning. This value becomes valid after reset only.

The maximum number of GVRP VLANs includes all the VLANs participating in GVRP operation regardless if they are static or dynamic.

The following should be considered when specifying the maximum number of VLANs participating in GVRP by setting the Maximum number of GVRP VLANs after Reset value:

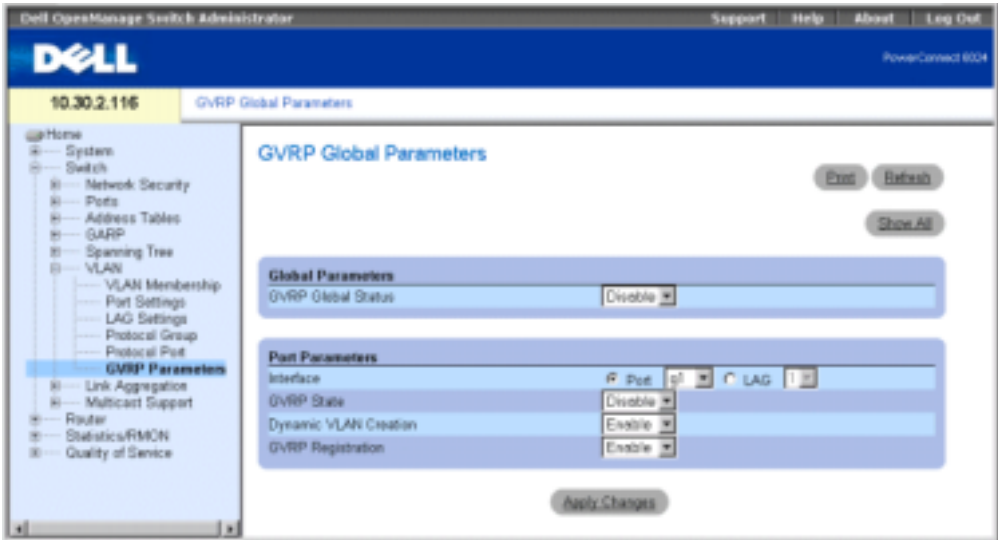
- The default maximum number of GVRP VLANs is equal to 255.
- The maximum number of VLANs (managed through Max VLANs MIB variable) limits the maximum number of GVRP VLANs.

To ensure the correct operation of the GVRP protocol, set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

- The number of all static VLANs both currently configured and expected to be configured.
- The number of all dynamic VLANs participating in GVRP both currently configured (initial number of dynamic GVRP VLANs is 255) and expected to be configured.

The **GVRP Global Parameters** page enables GVRP globally. You can also enable GVRP on a per-interface basis. To open the **GVRP Global Parameters** page, click **Switch→VLAN→GVRP Parameters** in the tree view.

Figure 7-33. GVRP Global Parameters Page



GVRP Global Status — Enables or disables GVRP on the device. GVRP is disabled by default.

Interface — The port or LAG for which GVRP is enabled.

GVRP State — Enables or disables GVRP on an interface.

Dynamic VLAN Creation — Enables or disables VLAN creation through GVRP.

GVRP Registration — Displays the GVRP Registration status.

Enabling GVRP On the Device

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field.
3. Click **Apply Changes**.

   GVRP is enabled on the device.

Enabling VLAN Registration Through GVRP

1. Open the **GVRP Global Parameters** page.
2. Select **Enable** in the **GVRP Global Status** field for the desired interface.
3. Select **Enable** in the **GVRP Registration** field.
4. Click **Apply Changes**.

   GVRP VLAN Registration is enabled on the port, and the device is updated.

Configuring GVRP Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring GVRP as displayed in the **GVRP Global Parameters** page.

Table 7-28. GVRP Global Parameters CLI Commands

CLI Command	Description
`gvrp enable (global)`	Enables GVRP globally.
`gvrp enable (interface)`	Enables GVRP on an interface.
`gvrp vlan-creation-forbid`	Enables or disables dynamic VLAN creation.
`gvrp registration-forbid`	De-registers all dynamic VLANs, and prevents dynamic VLAN registration on the port.
`show gvrp configuration [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays GVRP configuration information, including timer values, whether GVRP and dynamic VLAN creation is enabled, and which ports are running GVRP.
`show gvrp error-statistics [ethernet` *`interface`* `| port-channel` *`port-channel-number]`*	Displays GVRP error statistics.
`show gvrp statistics [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays GVRP statistics.
`clear gvrp statistics [ethernet interface | port-channel` *`port-channel-number`*`]`	Clears all the GVRP statistics information.

The following is an example of the CLI commands:

```
Console (config)# gvrp enable
Console (config)# interface ethernet g8
Console (config-if)# gvrp enable
Console (config-if)# gvrp vlan-creation-forbid
Console (config-if)# gvrp registration-forbid
Console> show gvrp configuration
GVRP Feature is currently Enabled on the device.
```

```
Maximum VLANs: 4063, Maximum VLANs after reset: 4063.

Port(s)  GVRP-Status Registration Dynamic VLAN Timers(milliseconds)
                                   Creation    Join      Leave      Leave All
-------- ---------- ------------ ------------  ----      -----      ---------
g1       Disabled    Normal       Enabled       200       600        10000
...
g7       Disabled    Normal       Enabled       200       600        10000
g8       Enabled     Forbidden    Disabled      200       600        10000
g9       Disabled    Normal       Enabled       200       600        10000
...
g24      Disabled    Normal       Enabled       200       600        10000
ch1      Disabled    Normal       Enabled       200       600        10000
...
ch7      Disabled    Normal       Enabled       200       600        10000
...
Console> show gvrp statistics


GVRP statistics:
----------------
Legend:
rJE  : Join Empty Received    rJIn : Join In Received
rEmp : Empty Received         rLIn : Leave In Received
rLE  : Leave Empty Received   rLA  : Leave All Received
sJE  : Join Empty Sent        sJIn : Join In Sent
sEmp : Empty Sent             sLIn : Leave In Sent
sLE  : Leave Empty Sent       sLA  : Leave All Sent
```

```
Port rJE  rJIn rEmp rLIn rLE  rLA  sJE  sJIn sEmp sLIn sLE  sLA
---  ---  ---- ---- ---- ---  ---  ---  ---  ---  ---- ---  ---
g1   0    0    0    0    0    0    0    0    0    0    0    0
g2   0    0    0    0    0    0    0    0    0    0    0    0
g3   0    0    0    0    0    0    0    0    0    0    0    0
g4   0    0    0    0    0    0    0    0    0    0    0    0
g5   0    0    0    0    0    0    0    0    0    0    0    0
g6   0    0    0    0    0    0    0    0    0    0    0    0
g7   0    0    0    0    0    0    0    0    0    0    0    0
g8   0    0    0    0    0    0    0    0    0    0    0    0
```

```
Console# clear gvrp statistics ethernet g8
```

Aggregating Ports

Link Aggregation optimizes port usage by linking a group of ports together to form a single LAG (aggregated group). Aggregating ports multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Your switch supports both static LAGs and Link Aggregation Control Protocol (LACP) LAGs. LACP LAGs negotiate aggregating ports' links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

The following guidelines should be followed when configuring Aggregating Ports:

- All ports within a LAG must be the same media type.
- A VLAN is not configured on the port.
- The port is not assigned to a different LAG.
- An available MAC address exists which can be assigned to a port.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in the LAG have the same ingress filtering and tagged modes.
- All ports in the LAG have the same back pressure and flow control modes.
- All ports in the LAG have the same priority.
- All ports in the LAG have the same transceiver type.

- PowerConnect 6024/6024F supports up to seven LAGs.
- Ports can be configured as LACP ports only if the ports are not part of a previously configured LAG.

Ports added to a LAG lose their individual port configuration. When ports are removed from the LAG, the original port configuration is applied to the ports.

Your switch uses a hash function to determine which packets are carried on which aggregated-link member. The hash function statistically load-balances the aggregated link members. The switch considers an Aggregated Link a single logical port.

To open the **Link Aggregation** page, click **Switch→Link Aggregation** in the tree view.

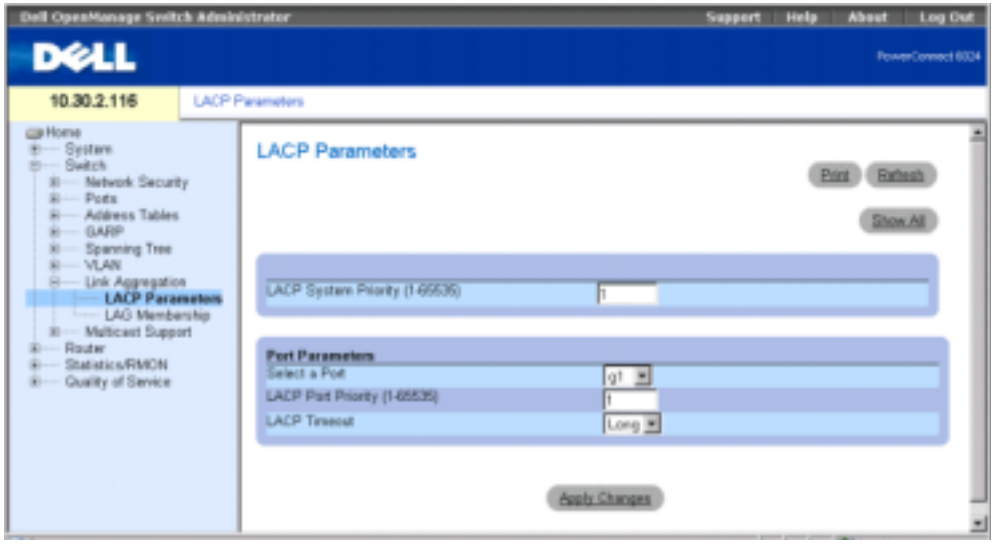
Defining LACP Parameters

Aggregate ports can be linked into link-aggregation port-groups. Each group is comprised of ports with the same speed, set to full-duplex operations.

Ports in a link aggregated group (LAG) can contain different media types if the ports are operating at the same speed. Aggregated links can be manually or automatically configured by enabling Link Aggregation Control Protocol (LACP) on the relevant links.

Use the **LACP Parameters** page to configure LACP LAGs. To open the **LACP Parameters** page, click **Switch→Link Aggregation→LACP Parameters** in the tree view.

Figure 7-34. LACP Parameters Page



The **LACP Parameters** page contains sections for defining global parameters and port parameters.

LACP System Priority (1-65535) — Indicates the LACP priority value for global settings. The default value is 1.

Select a Port — The port number to which timeout and priority values are assigned.

LACP Port Priority (1-65535) — LACP priority value for the port.

LACP Timeout — Administrative LACP timeout. Possible values are:

Short — Specifies a short timeout value.

Long — Specifies a long timeout value.

Defining Link Aggregation Global Parameters

1. Open the **LACP Parameters** page.
2. Complete the **LACP System Priority** and the **LACP Timeout** fields.
3. Click **Apply Changes**.

   The parameters are defined, and the device is updated.

Defining Link Aggregation Port Parameters

1. Open the **LACP Parameters** page.
2. Scroll to the **Port Parameters** table.
3. Select the port for which you want to define parameters.
4. Define the **LACP System Priority** and the **LACP Timeout** fields.
5. Click **Apply Changes**.

   The parameters are defined, and the device is updated.

Displaying the LACP Parameters Table

1. Open the **LACP Parameters** page.
2. Click **Show All** to display the **LACP Parameters Table**.

Configuring LACP Parameters Using CLI Commands

The following table summarizes the equivalent CLI commands for configuring LACP parameters as displayed in the **Link Aggregation** page.

Table 7-29. LACP Parameters CLI Commands

CLI Command	Description
`lacp system-priority` *`value`*	Configures the system priority.

Table 7-29. LACP Parameters CLI Commands

CLI Command	Description
`lacp port-priority` *`value`*	Configures the priority value for physical ports.
`lacp timeout {long | short}`	Assigns an administrative LACP timeout.
`show lacp ethernet` *`interface`* `[parameters | statistics | protocol-state]`	Displays LACP information for ethernet ports.

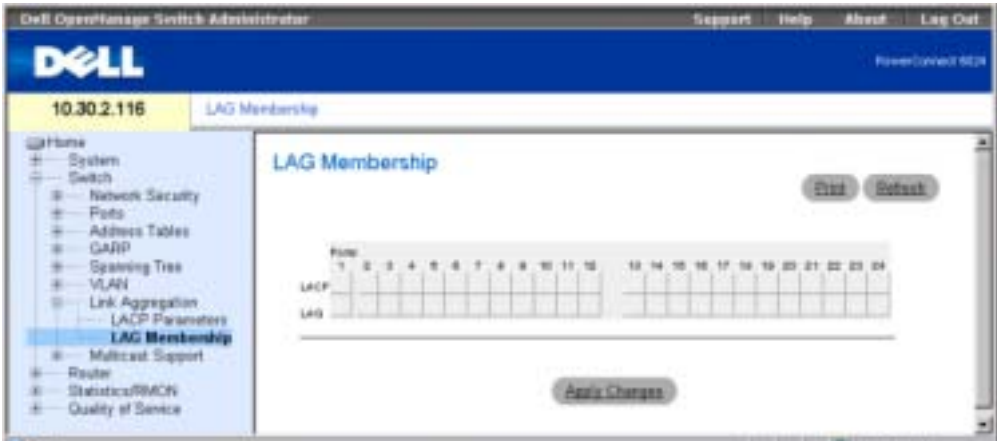
The following is an example of the CLI commands:

```
Console (config)# lacp system-priority 120
Console (config)# interface ethernet g8
Console (config-if)# lacp port-priority 247
Console (config-if)# lacp timeout long
Console (config-if)# exit
Console# show lacp ethernet g1 statistics
Port 1 LACP Statistics:
LACP PDUs sent:2
LACP PDUs received:2
```

Defining LAG Membership

Your switch supports seven LAG per system, and seven ports per LAG. Use the **LAG Membership** page to assign ports to LAGs. To open the **LAG Membership** page, click **Switch→Link Aggregation→LAG Membership** in the tree view.

Figure 7-35. LAG Membership Page



LACP — Aggregates the port to a LAG, using LACP.

LAG — Adds a port to a LAG, and indicates the specific LAG to which the port belongs.

Adding a Port to a LAG

1. Open the **LAG Membership** page.
2. Toggle the button under the port number to assign the static setting and the LAG number.
3. Toggle the button in the LACP row to **L** to aggregate the port to a LAG with LACP
4. Click **Apply Changes**.

   The port is added to the LAG, and the device is updated.

Assigning Ports to LAGs Using CLI Commands

The following table summarizes the equivalent CLI commands for assigning ports to LAGs as displayed in the **LAG Membership** page.

Table 7-30. LAG Membership CLI Commands

CLI Command	Description
`interface port-channel` *`port-channel-number`*	Enters the interface configuration mode of a specific port-channel.
`channel-group` *`port-channel-number`* `mode {on | auto}`	Associates a port with a port-channel. Use the no form of this command to remove the channel-group configuration from the interface

Table 7-30. LAG Membership CLI Commands

CLI Command	Description
`show interfaces port-channel [port-channel-number]`	Displays port-channel information.

```
Console (config)# interface port-channel 1
Console (config-if)# channel-group 1 mode on
Console# show interfaces port-channel
ChannelPort
------------        ----------------------------------
Ch 1                  Active    g1, g2   Inactive g3
Ch 2                  Active    g2
Ch 3                  Inactive  g8
```

Multicast Forwarding Support

Multicast forwarding allows a single packet to be forwarded to multiple destinations. The L2 Multicast service is based on an L2 switch receiving a single packet addressed to a specific Multicast address. Multicast forwarding creates copies of the packet, and transmits the packets to the relevant ports.

This device supports:

- **Forwarding L2 Multicast Packets** — Forwards Layer 2 Multicast packets. Layer 2 Multicast filtering is enabled by default and is not user-configurable.

NOTE: The system supports Multicast filtering for 256 Multicast groups.

- **Filtering L2 Multicast Packets** — Forwards Layer 2 packets to interfaces. If Multicast filtering is disabled, Multicast packets are flooded to all relevant ports.

To open the **Multicast Support** page, click **Switch→Multicast Support** in the tree view.

Defining Multicast Global Parameters

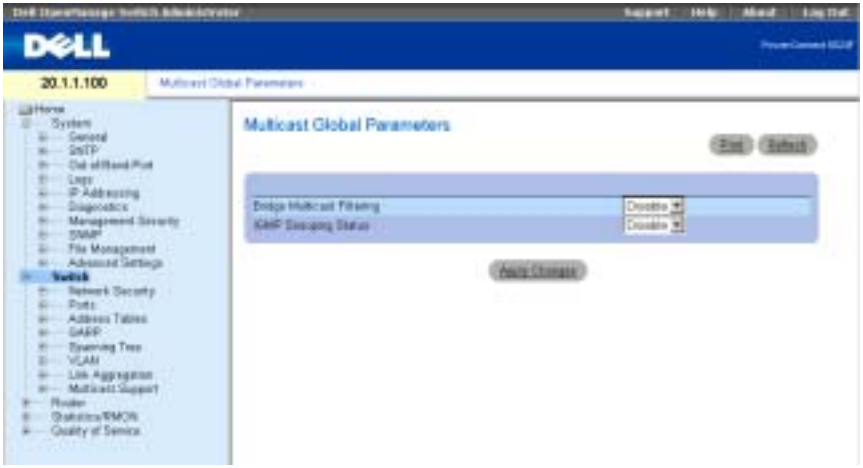
Layer 2 switching forwards Multicast packets to all relevant VLAN ports by default, managing the packet as a Multicast transmission. While Multicast traffic forwarding is effective, it is not optimal as irrelevant ports also receive the Multicast packets. The excess packets cause increased network traffic. Multicast forwarding filters enable forwarding of Layer 2 packets to port subsets.

When IGMP Snooping is enabled globally, all IGMP packets are forwarded to the CPU. The CPU analyzes the incoming packets and determines which ports want to join which Multicast groups, which ports have Multicast routers generating IGMP queries, and which routing protocols are forwarding packets and Multicast traffic.

Ports requesting to join a specific Multicast group issue an IGMP report specifying that the Multicast group is accepting members. This creates the Multicast filtering database.

Use the **Multicast Global Parameters** page to enable IGMP Snooping on the device. To open the **Multicast Global Parameters** page, click **Switch→Multicast Support→Global Parameters** in the tree view.

Figure 7-36. Multicast Global Parameters



The **Multicast Global Parameters** page contains the following fields:

Bridge Multicast Filtering — Enables or disables bridge Multicast filtering. Disabled is the default value.

IGMP Snooping Status — Enables or disables IGMP Snooping on the device. Disabled is the default value.

Enabling Bridge Multicast Filtering on the Device

1. Open the **Multicast Global Parameters** page.
2. Select **Enable** in the **Bridge Multicast Filtering** field.

3 Click **Apply Changes**.

Bridge Multicast is enabled on the device.

Enabling IGMP Snooping on the Device

1 Open the **Multicast Global Parameters** page.

2 Select **Enable** in the **IGMP Snooping Status** field.

3 Click **Apply Changes**.

IGMP Snooping is enabled on the device.

Enabling Multicast Forwarding and IGMP Snooping Using CLI Commands

The following table summarizes the equivalent CLI commands for enabling Multicast forwarding and IGMP Snooping as displayed on the **Multicast Support** page.

Table 7-31. Multicast Forwarding and Snooping CLI Commands

CLI Command	Description
`bridge multicast filtering`	Enables filtering of Multicast addresses.
`ip igmp snooping`	Enables Internet Group Membership Protocol (IGMP) snooping.

The following is an example of the CLI commands:

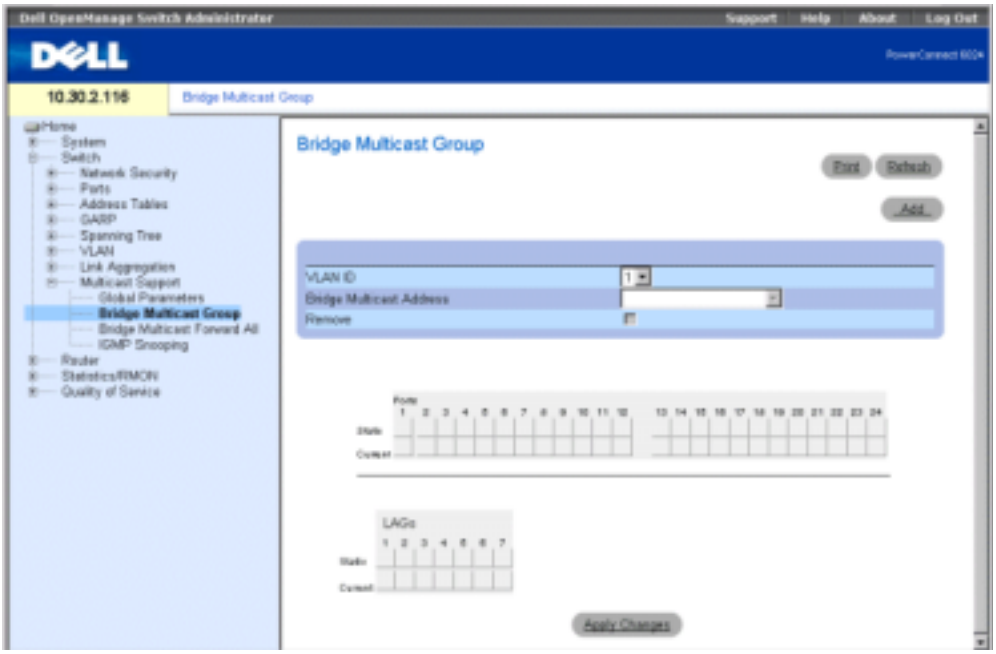
```
Console (config)# bridge multicast filtering
Console (config)# ip igmp snooping
```

Adding Bridge Multicast Address Members

The **Bridge Multicast Group** page displays the ports and LAGs attached to the Multicast service group in the **Ports** and **LAGs** tables. The Port and LAG tables also reflect the manner in which the port or LAGs joined the Multicast group. Ports can be added either to existing groups or to new Multicast service groups. The **Bridge Multicast Group** page permits new multicast service groups to be created. The **Bridge Multicast Group** page also assigns ports to a specific multicast service address group.

To open the **Bridge Multicast Group** page, click **Switch→Multicast Support→Bridge Multicast Address** in the tree view.

Figure 7-37. Bridge Multicast Group Page



VLAN ID — Identifies a VLAN and contains information about the multicast group address.

Bridge Multicast Address — Identifies the Multicast group MAC address/IP address.

Remove — When checked, removes a Bridge Multicast address.

Ports — Port that can be added to a Multicast service.

LAGs — LAGs that can be added to a Multicast service.

The following table contains the settings for managing IGMP port and LAG members.

Table 7-32. IGMP Port/LAG Members Table Control Settings

Port Control	Definition
D	Indicates that the port/LAG has joined the Multicast group dynamically in the *Current* Row.
S	Attaches the port to the Multicast group as static member in the *Static* Row.
	Indicates that the port/LAG has joined the Multicast group statically in the *Current* Row.
F	Indicates that the port/LAG is forbidden entry into the Multicast group.

Table 7-32. IGMP Port/LAG Members Table Control Settings

Port Control	Definition
Blank	Indicates that the port is not attached to a Multicast group.

Adding Bridge Multicast Addresses

1. Open the **Bridge Multicast Group** page.
2. Click **Add** to display the **Add Bridge Multicast Group** page.

Figure 7-38. Add Bridge Multicast Group Page

3. Define the **VLAN ID** and **New Bridge Multicast Address** fields.
4. Toggle a port to **S** to join the port to the selected multicast group.
5. Toggle a port to **F** to forbid adding specific multicast addresses to a specific port.
6. Click **Apply Changes**.

   The bridge multicast address is assigned to the multicast group, and the device is updated.

Defining Ports to Receive Multicast Service

1. Open the **Bridge Multicast Group** page.
2. Define the **VLAN ID** and the **Bridge Multicast Address** fields.
3. Toggle a port to **S** to join the port to the selected multicast group.
4. Toggle a port to **F** to forbid adding specific multicast addresses to a specific port.
5. Click **Apply Changes**.

   The port is assigned to the multicast group, and the device is updated.

Assigning LAGs to Receive Multicast Service

1. Open the **Bridge Multicast Group** page.
2. Define the **VLAN ID** and the **Bridge Multicast Address** fields.
3. Toggle the LAG to **S** to join the LAG to the selected multicast group.
4. Toggle the LAG to **F** to forbid adding specific multicast addresses to a specific LAG.
5. Click **Apply Changes**.

   The LAG is assigned to the multicast group, and the device is updated.

Managing Multicast Service Members Using CLI Commands

The following table summarizes the equivalent CLI commands for managing Multicast service members as displayed in the **Bridge Multicast Group** page.

Table 7-33. Multicast Service Member CLI Commands

CLI Command	Description
`bridge multicast address {`*`mac-multicast-address`* `|` *`ip-multicast-address`*`} [add | remove] {ethernet` *`interface-list`* `| port-channel` *`port-channel-number-list`* `}`	Registers MAC-layer multicast addresses to the bridge table, and adds static ports to the group.
`bridge multicast forbidden address {`*`mac-multicast-address`* `|` *`ip-multicast-address`*`} [add | remove] {ethernet` *`interface-list`* `| port-channel` *`port-channel-number-list`*`}`	Forbids adding a specific multicast address to specific ports. Use the no form of this command to return to default
`show bridge multicast address-table [vlan` *`vlan-id`*`] [address` *`mac-multicast-address`* `|` *`ip-multicast-address`*`] [format ip | mac]`	Displays Multicast MAC address table information.

The following is an example of the CLI commands:

```
console#config
console(config)#vlan database
console(config-if)#vlan 8
console(config-if)#exit
```

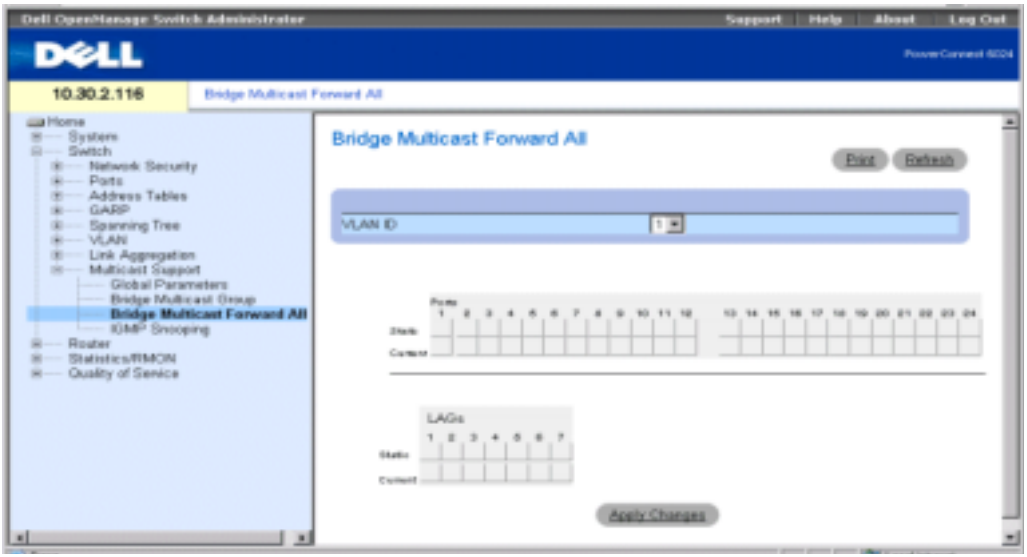
```
console(config)#interface range ethernet g1-9
console(config-if)# switchport mode general
console(config-if)# switchport general allow vlan add 8
console(config)#interface vlan 8
Console(config-if)# bridge multicast address 0100.5e02.0203
add ethernet g1-9
Console(config-if)# exit
Console(config)# exit
Console# show bridge multicast address-table
Vlan MAC Address    type     Ports
---- -------------- -----    -----------
1    0100.5e02.0203 static   g1, g2
19   0100.5e02.0208 static   g1-8
19   0100.5e02.0208 dynamicg 9-11
Forbidden ports for multicast addresses:
Vlan MAC Address  Ports
-----------------------------------
1   0100.5e02.0203  g8
19  0100.5e02.0208  g8
Console# configuration
Console (config)# interface vlan 8
Console (config-if)# bridge multicast address 0100.5e02.0203
Console (config-if)# bridge multicast forbidden address
0100.5e02.0203 add ethernet g9
```

Assigning Multicast Forward All Parameters

Use the **Bridge Multicast Forward All** page to enable attaching ports or LAGs to a switch that is attached to a neighboring Multicast router/switch. Once IGMP Snooping is enabled, multicast packets are forwarded to the appropriate port or VLAN.

To open the **Bridge Multicast Forward All** page, click **Switch→Multicast Support→Bridge Multicast→Bridge Multicast Forward All** in the tree view.

Figure 7-39. Bridge Multicast Forward All Page



VLAN ID — Identifies a packet VLAN and contains information about the multicast group address.

Ports — Ports that can be added to a multicast service.

LAGs — LAGs that can be added to a multicast service.

The following table contains the settings for managing router and port settings.

Table 7-34. Bridge Multicast Forward All Router/Port Control

Port Control	Definition
D	Attaches the port to the Multicast router or switch as a dynamic port.
S	Attaches the port to the Multicast router or switch as a static port.
F	Forbidden
Blank	Indicates that the port is not attached to a Multicast router or switch.

Attaching a Port to a Multicast Router or Switch

1. Open **Bridge Multicast Forward All** page.
2. Define the **VLAN ID** field.
3. Select a port in the **Ports** table, and assign the port a value.

4 Click **Apply Changes**.

The port is attached to the multicast router or switch.

Attaching a LAG to a Multicast Router or Switch

1 Open **Bridge Multicast Forward All** page.

2 Define the **VLAN ID** field.

3 Select a port in the **LAGs** table, and assign the LAG a value.

4 Click **Apply Changes**.

The LAG is attached to the multicast router or switch.

Managing LAGs and Ports Attached to Multicast Routers Using CLI Commands

The following table summarizes the equivalent CLI commands for managing LAGs and ports attached to Multicast routers as displayed on the **Bridge Multicast Forward All** page.

Table 7-35. CLI Commands for Managing LAGs and Ports Attached to Multicast Routers

CLI Command	Description
`show bridge multicast filtering` *`vlan-id`*	Displays the multicast filtering configuration.
`bridge multicast forward-all {add | remove} {ethernet` *`interface-list`* `| port-channel` *`port-channel-number-list`*`}`	Enables forwarding of all multicast packets on a port. Use the no form of this command to return to default.

The following is an example of the CLI commands:

```
Console# show bridge multicast filtering 1

Filtering: Disabled

VLAN: 1

Forward-All

Port      Static         Status

------    ---------      ---------

g1        -              Filter

g2        -              Filter

...
```

```
console#config
console(config)#vlan database
console(config-if)#vlan 8
console(config-vlan)#exit
console(config)#interface range ethernet g1-9
console(config-if)# switchport mode general
console(config-if)# switchport general allow vlan add 8
console(config)#interface vlan 8
Console(config-if)# bridge multicast address 0100.5e02.0203
add ethernet g1-9
Console(config-if)# exit
Console(config)# exit
Console# configuration
Console (config)# interface VLAN 1
Console (config-if)# bridge multicast forward-all add ethernet g8
```

IGMP Snooping

Use the **IGMP Snooping** page to add IGMP members. To open the **IGMP Snooping** page, click **Switch→Multicast Support→IGMP Snooping** in the tree view.

Figure 7-40. IGMP Snooping

VLAN ID — Specifies the VLAN ID.

IGMP Snooping Status — Enables or disables IGMP snooping on the VLAN.

Auto Learn — Enables or disables Auto Learn on the device.

Host Timeout (1-2147483647) — Time before an IGMP snooping entry is aged out. The default time is 260 seconds.

Multicast Router Timeout (1-2147483647) — Time before aging out a Multicast router entry. The default value is 300 seconds.

Leave Timeout (0-2147483647) — Time, in seconds, after a port leave message is received before the entry is aged out. **User-defined** enables you to set the timeout period, and **Immediate Leave** specifies an immediate timeout period. The default timeout is 10 seconds.

Enabling IGMP Snooping on the Device

1. Open the **IGMP Snooping** page.
2. Select the VLAN ID for the device on which you want to enable IGMP snooping.
3. Select **Enable** in the **IGMP Snooping Status** field.
4. Complete the fields on the page.
5. Click **Apply Changes**.

   IGMP snooping is enabled on the device.

Displaying the IGMP Snooping Table

1. Open the **IGMP Snooping** page.

2 Click **Show All** to display the **IGMP Snooping Table**.

Configuring IGMP Snooping with CLI Commands

The following table summarizes the equivalent CLI commands for configuring locked port security as displayed in the **IGMP Snooping** page.

Table 7-36. IGMP Snooping CLI Commands

CLI Command	Description
`ip igmp snooping`	Enables Internet Group Membership Protocol (IGMP) snooping.
`ip igmp snooping mrouter learn-pim-dvmrp`	Enables automatic learning of multicast router ports in the context of a specific VLAN.
`ip igmp snooping host-time-out` *`time-out`*	Configures the host-time-out.
`ip igmp snooping mrouter-time-out` *`time-out`*	Configures the mrouter-time-out.
`ip igmp snooping leave-time-out {`*`time-out`*` | immediate-leave}`	Configures the leave-time-out.
`show ip igmp snooping interface` *`vlan-id`*	Displays IGMP snooping configuration.
`show ip igmp snooping mrouter [interface` *`vlan-id`*`]`	Displays information about dynamically learned Multicast router interfaces.

The following is an example of the CLI commands:

```
Console (config)# ip igmp snooping
Console (config)# interface vlan 1
Console (config-if)# ip igmp snooping mrouter learn-pim-dvmrp
Console (config-if)# ip igmp snooping host-time-out 300
Console (config-if)# ip igmp snooping mrouter-time-out 200
Console (config-if)# exit
Console (config)# interface vlan 1
Console (config-if)# ip igmp snooping leave-time-out 60
Console (config-if)# exit
```

```
Console (config)# exit
Console # show ip igmp snooping interface 1000
IGMP Snooping is globally enabled
IGMP Snooping is enabled on VLAN 1000
IGMP host timeout is 300 sec
IGMP Immediate leave is disabled. IGMP leave timeout is 10 sec
IGMP mrouter timeout is 200 sec
Automatic learning of multicast router ports is enabled
Console> show igmp-snooping mrouter
VLAN     Ports
-------  ----------------------------------------
2        g9
```

8

Configuring Routing

Routing Overview

Devices in different subnetworks communicate with each other using a Layer 3 router between the VLANs. Routing is enabled by default on your switch. However, at least one IP interface must be configured for the switch to begin routing network traffic. Routes are either statically configured, or are configured using Routing Information Protocol (RIP) or Open Shortest Path First (OSPF).

For more information about RIP, see "Configuring RIP."

For more information about OSPF, see "Configuring OSPF Parameters and Filters."

Configuring Global IP Routing

The **Global Routing Parameters** page contains links for configuring routing. Routing is always on, but it is only enabled if the system has one or more IP addresses. To open the **Global Routing Parameters** page, click **Router→Global Routing Parameters** in the tree view.

This **Global Routing Parameters** page contains links that allow you to perform the following procedures:

- Configuring the IP Forwarding Table.
- Configuring IP Static Routes.
- Configuring VRRP.
- Configuring MD5 Routing Authentication.
- Configuring MD5 Key Chain Settings.

Configuring the IP Forwarding Table

Use the **IP Forwarding** page to view the routing parameters by which IP traffic is forwarded. This page provides a list of IP routes for selected destination IP addresses, including IP routes that are defined statically or dynamically. IP routes are based on network masks, next hops, metrics, and forwarding protocols. These parameters determine how specific packets are forwarded or dropped. When an IP address is configured on an interface, it is included in the IP Forwarding Table.

To open the **IP Forwarding** page, click **Router→Global Routing Parameters→IP Forwarding** in the tree view.

Figure 8-1. IP Forwarding Page

Maximum Equal Cost Multipaths (ECMP) — The ECMP value, which must be defined when forwarding IP packets. The ECMP value indicates how many paths from the router to a network are available. The possible value range is 1-4. For example, a value of 1 indicates that there is only one path to the network. The higher the value, the more memory resources are required. Modifications to this field are effective only after the device is reset.

Destination IP Address — The destination IP network.

Prefix Length — The number of bits that comprise the destination IP address prefix. The length is between 1-32 bits.

Next Hop (Gateway) — The next router address on the route to the destination network.

Route Type—Specifies how remote routing is handled. Possible values are:

Remote — Packet is forwarded.

Reject — Packet is dropped.

Local — Packet is sent to a local network.

Metric — The number of hops to the destination network.

Protocol — Routing protocol by which this route was added.

Displaying the IP Forwarding Table

The **IP Forwarding Table** provides a list of all IP routes in the system.

1. Open the **IP Forwarding** page.
2. Click **Show All** to display the **IP Forwarding Table**.

Viewing IP Forwarding Using the CLI Commands

The following table contains the CLI commands for viewing IP Forwarding.

Table 8-1. IP Forwarding CLI Commands

CLI Command	Description
`show ip route [address]<ip-address>`	Displays the current state of the routing table.
`ip maximum-paths number-paths`	Controls the maximum number of parallel routes installed in a routing table.

The following is an example of the CLI commands:

```
Console (config)# interface ip 10.10.10.2

Console (config-ip)# ip maximum-paths 2

Console (config-ip)# exit

Console (config)# exit

Console# exit

Console> show ip route

Codes: C - connected, S - static, R - RIP, O - OSPF, E - OSPF
external

R 10.0.0.0/8 is rejected

C 10.0.1.1/32 is directly connected, Loopback0

C 10.0.1.0/24 is directly connected, Ethernet g1

C 10.0.2.0/24 is directly connected, Ethernet g2

R 10.8.2.0/24 [230/50] via 10.0.2.2, 00:17:19, Ethernet g2

S 10.9.1.0/24 [5/2] via 10.0.1.2, 17:19:18, Ethernet g1

S 10.9.1.0/24 [5/3] via 10.0.2.2, Backup Not Active

O 10.8.1.0/24 [30/2000] via 10.0.1.2, 00:39:08, Ethernet g1

S 172.1.0.0/16 [5/3] via 10.0.1.1, 18:21:58, Ethernet g1

S 172.1.1.0/24 [5/3] via 10.0.2.1, 17:12:19, Ethernet g1

S 172.1.1.1/32 [5/3] via 10.0.3.1, 19:51:18, Ethernet g1

Maximum Parallel Paths: 2
```

Configuring IP Static Routes

Use the IP Static Route page to define static routes.

To open the IP Static Route page, click **Router→Global Routing Parameters→IP Static Route** in the tree view.

Figure 8-2. IP Static Route Page

Destination IP Address — Static route's destination IP network.

Network Mask—The destination network mask for this route.

Prefix Length — The number of bits that comprise the destination IP address prefix. The length is between 1-32 bits.

Next Hop — Indicates the next system address on the route.

Route Type — Specifies how remote routing is handled. The possible field values are:

Remote — Packet is forwarded.

Reject — Packet is dropped.

Local — Packet is sent to a local network.

Metric (1-255)— Number of hops to the destination network.

Adding Static IP Routes

NOTE: Only a directly connected router can be defined as a gateway.

1 Open the **IP Static Route** page.

2 Define the fields on the page.

NOTE: Selecting a **Route Type** of **Reject** ensures routes to the designated network inaccessible.

To define a static route to a host located on a remote network, select **Remote** for **Route Type**.

To define a static route to a host located on the local network, select **Local** for **Route Type**.

The **Destination IP Address** and **Network Mask** designates the remote network address. **The Next Hop** is the address of a router directly connected to your switch.

The **Destination IP Address** is the address of the host. The **Next Hop** should be filled in as 0.0.0.0.

3 Click **Apply Changes**.

The new static route is added, and the device is updated.

Removing an IP Static Route

1 Open the **IP Static Route** page.

2 Click **Show All** to display the **IP Static Route Table**.

3 Check **Remove for the Destination IP address** of the static route you want to remove.

4 Click **Apply Changes**.

The static route is deleted, and the device is updated.

Configuring the IP Static Table Using the CLI Commands

The following table contains the CLI commands for configuring the IP Static Table.

Table 8-2. IP Static Route Table CLI Commands

CLI Command	Description
`ip route` *`prefix`* `{`*`mask`* `|` *`prefix-length`*`}` *`gateway`* `[metric` *`distance`*`] [reject-route]`	Establishes static IP routes.

The following is an example of the CLI commands:

```
Console (config)# ip route 172.16.0.0 255.255.0.0  131.16.1.1
```

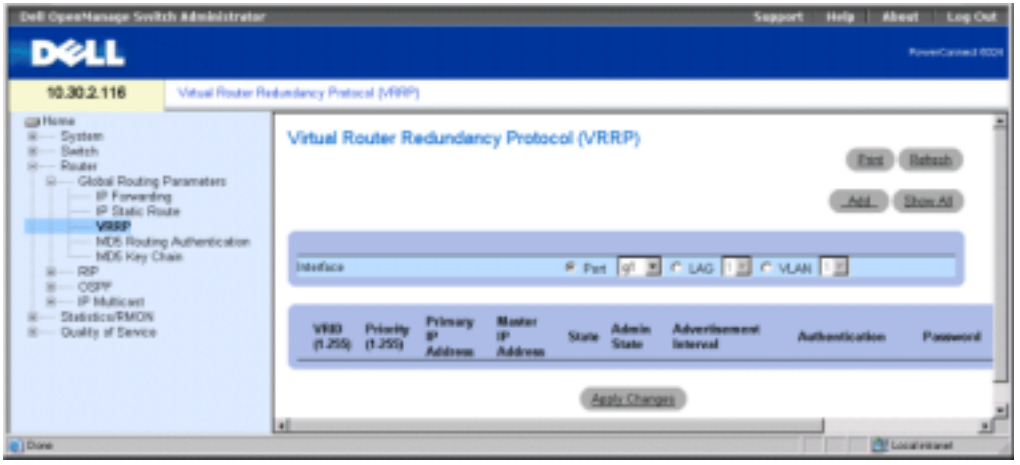
Configuring VRRP

Virtual Router Redundancy Protocol (VRRP) specifies an elector protocol that dynamically assigns routing responsibility to one of the VRRP routers on the LAN (the master router). The election process enables dynamic failover of routing responsibility in case the master router becomes unavailable.

The advantage of VRRP is that it eliminates the single-point-failure phenomenon inherent to the routing environment by providing a higher availability default path, while eliminating the need for configuration of dynamic routing or router discovery protocols on every end-host.

The **Virtual Router Redundancy Protocol (VRRP)** page sets the switch's VRRP routing parameters. To open the **Virtual Router Redundancy Protocol (VRRP)** page, click **Router** → **Global Routing Parameters**→**VRRP** in the tree view.

Figure 8-3. Virtual Router Redundancy Protocol (VRRP) Page



Interface — Interface type and number attached to the VRRP router.

VRID (1-255) — Virtual router identifier.

Priority (1-255) — Router priority used for the virtual router election process. The value may determine if a higher priority VRRP router overrides a lower priority VRRP router.

Primary IP Address — Virtual IP address identified with the virtual router. The primary IP Address is selected from actual interface addresses configured on a VRRP router.

Master IP Address — The VRRP router that is currently master for this virtual router.

State — The current router state. Possible values are:

> **Master** — The router functions as the forwarding router for the IP addresses associated with the virtual router. The master router responds to ARP requests with associated IP addresses in the ARP target, forwards packets with Virtual MAC Address (VMAC) as the destination

MAC, and accepts packets associated with the virtual IP addresses (only if the router owns the associated IP address).

Initialize — The router waits for a startup event. When the startup event is received, the router transits to the appropriate state.

Backup — The router backs up to the master router. The router continuously monitors if the master router is available by the periodic advertisements the master sends or by specific advertisements sent from the master announcing that it is going down.

Admin State — Indicates if the router is up or down.

Advertisement Interval—Indicates the rate at which advertisements are sent when the router is the master.

Authentication — Specifies if no authentication process takes place, or if passwords are used to authenticate VRRP protocol exchanges.

Password — The password used to authenticate VRRP protocol exchanges.

Preempt — When checked, allows higher priority VRRP routers to override lower priority routers.

Remove — When checked, removes VRRP entries from the VRRP Table.

Adding Routers to a VRRP Group

1. Open the **Virtual Router Redundancy Protocol (VRRP)** page.
2. Click **Add** to display the **Add VRRP Interface** page.

Figure 8-4. Add VRRP Interface

3 Define the fields.

See "Configuring VRRP" for information about the fields.

NOTE: VRRP interfaces must be defined before the admin state can be *Enabled*.

4 Click **Apply Changes**.

The new VRRP interface is added, and the device is updated.

NOTE: If an illegal virtual IP address is entered, a warning will display, but the virtual router will be added. It is recommended that you delete this entry from the virtual routers table.

Modifying VRRP Routers

1 Open the **Virtual Router Redundancy Protocol (VRRP)** page.

2 Select an interface in the **Interface** field.

3 Define the fields as desired.

4 Click **Apply Changes**.

Deleting a VRRP Entry

1 Open the **Virtual Router Redundancy Protocol (VRRP)** page.

2 Click **Show All** to display the **VRRP Table**.

3 Select a table entry.

4 Check the **Remove** check box.

5 Click **Apply Changes**.

The VRRP entry is deleted, and the device is updated.

Configuring VRRP Using the CLI Commands

The following table contains the CLI commands for configuring the VRRP.

Table 8-3. VRRP CLI Commands

CLI Command	Description
`vrrp virtual-router ip ip-address [ip-address2…ip-address8]`	Defines Virtual Router Redundancy Protocol (VRRP) for an interface.
`vrrp virtual-router up`	Activates Virtual Router Redundancy Protocol (VRRP) on an interface.
`vrrp virtual-router timer seconds`	Configures the time interval between sending advertisements messages.
`vrrp virtual-router priority priority`	Configures Virtual Router Redundancy Protocol (VRRP) priority on an interface.

Table 8-3. VRRP CLI Commands

CLI Command	Description
`vrrp virtual-router source-ip ip-address`	Defines the source IP address (primary IP address) used for Virtual Router Redundancy Protocol (VRRP) messages on an interface.
`vrrp virtual-router authentication text`	**Enables authentication for the Virtual Router Redundancy Protocol (VRRP) on an interface.**
`vrrp virtual-router preempt`	Enables the Virtual Router Redundancy Protocol (VRRP) preemption on an interface.
`show vrrp configuration [ethernet interface-number | vlan vlan-id | port-channel number]`	Displays the Virtual Router Redundancy Protocol (VRRP) configuration.
`show vrrp status [ethernet interface-number | vlan vlan-id | port-channel number]`	Displays Virtual Router Redundancy Protocol (VRRP) status.

Configuring VRRP Using the CLI Commands

The following is an example of the CLI commands:

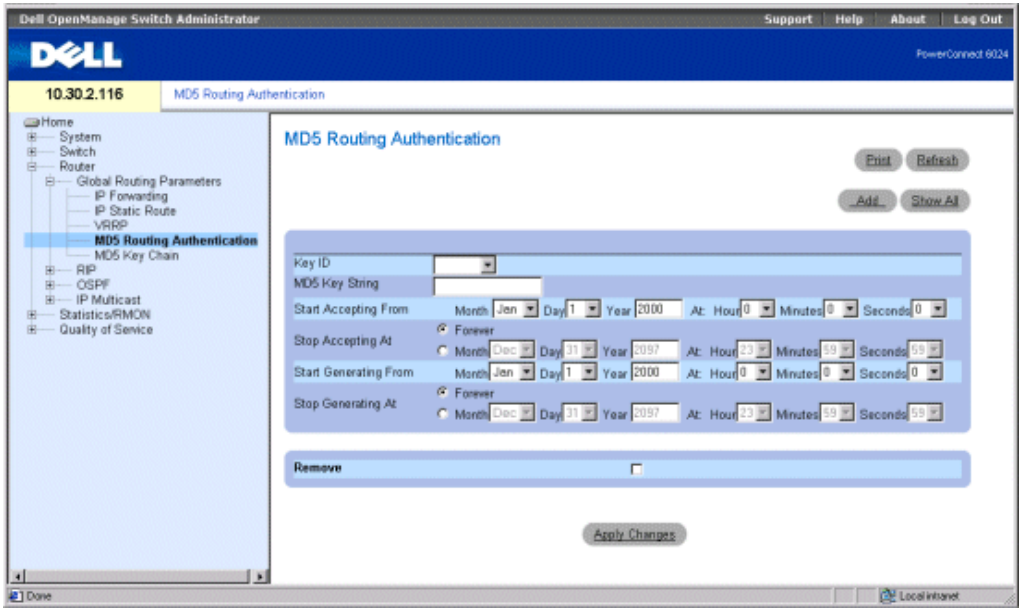
```
Console(config)# interface ethernet g8
Console(config-if)# vrrp 45 ip 172.16.1.1 172.16.2.1
Console(config-if)# vrrp 45 up
Console(config-if)# vrrp 45 timer 100
Console(config-if)# vrrp 45 priority 150
Console(config-if)# vrrp 45 source-ip 168.192.1.1
Console(config-if)# vrrp 45 authentication Dell
Console(config-if)# vrrp 45 preempt
Console(config-if)# exit
Console(config)# exit
```

Configuring MD5 Routing Authentication

MD5 keys are used by the Message Digest-5 Authentication Algorithm. Start and end times, for both sending and receiving, can be defined for each key. Keys that are active and expire at the reset times can be configured. Interfaces that are inter-communicating must have the same Key ID. If key times overlap on the send side, the device uses the key with the latest start time. When receiving packets, the interface uses the key indicated by the **Key ID** value on the packet.

Use the **MD5 Routing Authentication** page to define and manage keys. To open the **MD5 Routing Authentication** page, click **Router→Global Routing Parameters→MD5 Routing Authentication** in the tree view.

Figure 8-5. MD5 Routing Authentication



Key ID — Specifies the Key ID.

MD5 Key String — Indicates the password used for routing authentication.

Start Accepting From — Date and time the MD5 key begins accepting traffic with the specified MD5 key. The **Start Accept** field format is **Month Day Year At: Hour Minute Second**.

Stop Accepting At — Date and time the MD5 key begins no longer accepting traffic with the specified MD5 key. The **Stop Accept** field format is **Month Day Year At: Hour Minute Second**. If **Forever** is selected, no limit is set for accepting traffic with MD5 keys.

Start Generating From — Date and time the protocol packets are forwarded with MD5 keys. The **Start Generate** field format is **Month Day Year At: Hour Minute Second**.

Stop Generating At — Date and time the protocol packets are no longer forwarded with MD5 keys. The **Stop Generate** field format is **Month Day Year At: Hour Minute Second**. If **Forever** is selected, no limit is set for accepting traffic with MD5 keys.

Remove — When checked, removes the MD5 key.

Adding an MD5 Key

1. Open the **MD5 Routing Authentication** page.
2. Click **Add** to display the **Add MD5 Key** page.

Figure 8-6. Add MD5 Key

3. Define the fields in the dialog.
4. Click **Apply Changes**.

   The new MD5 key is added to the **MD5 Key Table**, and the device is updated.

Modifying an MD5 Key

1. Open the **MD5 Routing Authentication** page.
2. From the **Entry No.** drop-down menu, select the MD5 key you want to modify.
3. Modify the fields in the dialog.
4. Click **Apply Changes**.

   The new MD5 key is modified, and the device is updated.

Deleting an MD5 Key

1. Open the **MD5 Routing Authentication** page.
2. Click **Show All** to display the **MD5 Key Table**.

3 Select an entry in the **Key ID** field.

4 Check the **Remove** check box.

5 Click **Apply Changes**.

The MD5 Key is deleted, and the device is updated.

Configuring MD5 Authentication Using the CLI Commands

The following table contains the CLI commands for configuring MD5 Authentication.

Table 8-4. MD5 Authentication CLI Commands

CLI Command	Description
`key` *`key-id`*	Creates an authentication key.
`accept-lifetime { duration time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start key-lifetime-duration-in-seconds } | { infinite time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start } | { time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start time-to-stop day-of-the-month` *`day-of-the-month`* `year-to-stop }`	Sets the time period during which the authentication key on a key chain can be received.
`send-lifetime { duration time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start key-lifetime-duration-in-seconds } | { infinite time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start } | { time-to-start day-of-the-month` *`day-of-the-month`* `year-to-start time-to-stop day-of-the-month` *`day-of-the-month`* `year-to-stop }`	Sets the time period during which an authentication key on a key chain can be sent.

The following is an example of the CLI commands:

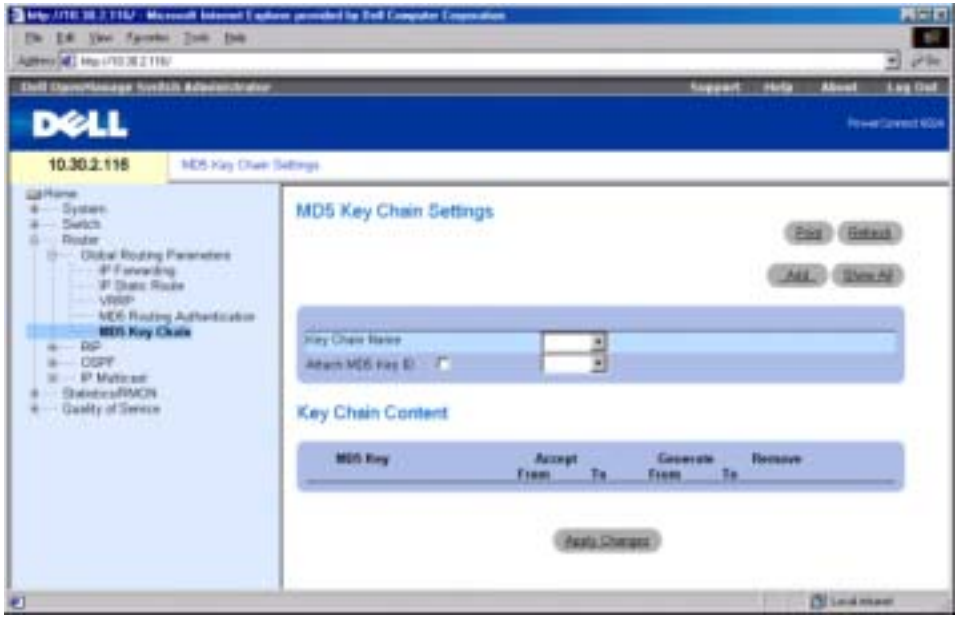
```
Console (config)# key 3

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25
2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002
3600
```

Configuring MD5 Key Chain Settings

After keys are defined, they are grouped into what is called a "key chain." Each router interface can be assigned several keys at once. Keys can be grouped into key chains for convenient assignment to interfaces. Each key can be included in several key chains. Key chains are assigned to interfaces in the RIP or OSPF interface parameters. MD5 keys are added to a MD5 key chain to generate the key chain.

Use the **MD5 Key Chain Settings** page to define key chains and assign keys to them. To open the **MD5 Key Chain Settings** page, click **Router→Global Routing Parameters→MD5 Key Chain** in the tree view.

Figure 8-7. MD5 Key Chain Settings



Key Chain Name — User-defined key chain names.

Attach MD5 Key ID—Indicates the key string ID attached to the Key Chain.

MD5 Key — The key that is a key chain member.

Accept From — Date and time the selected MD5 key begins accepting traffic with the specified MD5 key. The **Accept From** field format is **Month Day Year At: Hour Minute Second**. The **Accept From** field is the key defined in the **MD5 Routing Authentication** page.

Accept To — Date and time when the selected MD5 key no longer accepts traffic with the specified MD5 key. The field format is **Month Day Year At: Hour Minute Second**. The **Accept To** field is the key defined in the **MD5 Routing Authentication** page.

Generate From — Date and time the selected MD5 key begins forwarding traffic. The **Generate From** field format is **Month Day Year At: Hour Minute Second**. The **Generate From** field is the key defined in the **MD5 Routing Authentication** page.

Generate To — Date and time the selected MD5 key stops forwarding traffic. The **Generate To** field format is **Month Day Year At: Hour Minute Second**. The **Generate To** field is the key defined in the **MD5 Routing Authentication** page.

Remove — When checked, removes MD5 key from the MD5 Key Chain Table.

Adding an MD5 Key Chain

1. Open the **MD5 Key Chain Settings** page.
2. Click **Add** to display the **Add Key Chain** page.
3. Complete the **New Key Chain Name** and **Attach MD5 Key No.** fields.
4. Click **Apply Changes**.

   The new MD5 key chain is added to the MD5 Key Chain Table, and the device is updated.

Modifying an MD5 Key Chain

1. Open the **MD5 Key Chain Settings** page.
2. Modify the **Name** and/or the **Key Chain ID** fields.
3. Click **Apply Changes**.

   The new MD5 key chain is modified, and the device is updated.

Removing an MD5 Key Chain:

1. Open the **MD5 Key Chain Settings** page.
2. Click **Show All** to display the **MD5 Key Chain Table**.
3. Select an entry in the **Key Chain Name** field.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The MD5 key chain is removed, and the device is updated.

Configuring Key Chains Using CLI Commands

The following table contains the CLI commands for configuring the key chains.

Table 8-5. Key Chain CLI Commands

CLI Command	Description
`key-chain` *name-of-chain*	Identifies an authentication key group.
`key` *key-id*	Identifies an authentication key on a key chain.
`key-string` *text*	Specifies an authentication string for a key.
`accept-lifetime` *start-time end-time* | {`infinite` | *start-time* | `duration` *start-time seconds*} `no accept-lifetime`	Sets the time period during which the authentication key is valid for authenticating incoming packets.
`send-lifetime` *start-time end-time* | {`infinite` | *start-time* | `duration` *start-time seconds*}`no send-lifetime`	Sets the time period during which an authentication key is valid to generate an MD5 digest for outgoing packets.
`show key-chains` [*name-of-chain*]	Displays key chain information.

The following is an example of the CLI commands:

```
Console (config)# key chain M

Console (config-key-chain)# key 1

Console (config-key)# key-string mountain

Console (config-key)# accept-lifetime duration 13:30:00 Jan 25
2002 7200

Console (config-key)# send-lifetime duration 14:00:00 Jan 25 2002
3600

Console (config-key)# exit

Console (config)# exit

Console# show key-chains
```

```
key chain internal
key 1
accept:   13:30:00 Jan 25 2002 duration 7200
send:     14:00:00 Jan 25 2002 duration 3600
key 2
accept:14:30:00 Jan 25 2002 duration 7200
send:15:00:00 Jan 25 2002 duration 3600
key chain external
key 1
accept:13:30:00 Jan 25 2002 until 15:30:00 Jan 25 2002
send:14:00:00 Jan 25 2002 until 15:00:00 Jan 25 2002
key 2
accept:14:30:00 Jan 25 2002 until 16:30:00 Jan 25 2002
send:15:00:00 Jan 25 2002 until 16:00:00 Jan 25 2002
25 2002
```

Configuring RIP

Routing Information Protocol (RIP) is the most commonly used Internet standard for interior gateway protocols. The protocol broadcasts routing information to determine the quickest route to the next destination. RIP is a distance vector routing protocol that is best used in small networks. Routes are determined through the smallest hop count. Routing updates contain pairs of values consisting of an IP address and the distance to the node.

RIP version 2 does the following:

- Supports subnet masks.
- Provides authentication methods.
- Supports routing protocols.
- Provides larger distribution and smaller bandwidth overhead requirements.

You configure RIP on the **RIP** page. To open the **RIP** page, click **Router→RIP** in the tree view.

Defining RIP Global Parameters

The **RIP Global Parameters** page provides fields for enabling RIP on the device, establishing redistribution of OSPF and redistribution of static routes.

Click **Router→RIP→Global Parameters** in the tree view to display the **RIP Global Parameters** page.

Figure 8-8. RIP Global Parameters Page

RIP Status — Enables or disables RIP on the device.

Redistribute OSPF Routes — When enabled, redistributes routes from OSPF to RIP. Redistribution of routes involves importing foreign routing interfaces to RIP.

Redistribute Static Routes — When enabled, redistributes routes from static routes to RIP.

Enabling RIP, Redistribution of OSPF Routes, Redistribution of Static Routes

1. Open the **RIP Global Parameters** page.
2. Select **Enabled** in the RIP global parameter field that you want to enable.
3. Click **Apply Changes**.

   RIP is enabled on the device.

Configuring RIP Global Parameters Using CLI Commands

The following table contains the CLI commands for configuring the RIP global parameters.

Table 8-6. RIP Global Parameter CLI Commands

CLI Command	Description
`router rip enable`	Enables the Routing Information Protocol (RIP) on the device.
`no router rip enable`	Disables the Routing Information Protocol (RIP) on the device.

Table 8-6. RIP Global Parameter CLI Commands

CLI Command	Description
`router rip redistribute ospf`	Advertises routes learned by OSPF in the RIP process.
`no router rip redistribute ospf`	Stops advertisement of routes learned by OSPF in the RIP process.
`router rip redistribute static`	Advertises routes statically configured in the RIP process.
`no router rip redistribute static`	Stops advertisement of routes statically configured in the RIP process.

The following is an example of the CLI commands:

```
Console (config)# router rip enable
Console (config)# router rip redistribute ospf
Console (config)# router rip redistribute static
Console (config)# no router rip enable
Console (config)# no router rip redistribute ospf
Console (config)# no router rip redistribute static
```

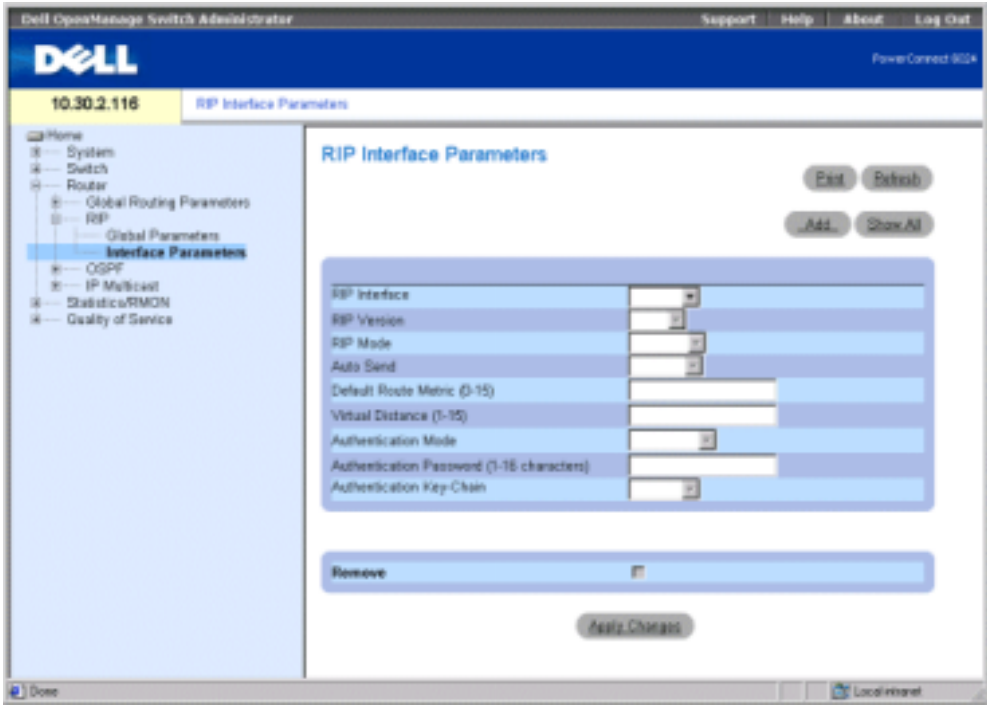
Defining RIP Interface Parameters

Use the **RIP Interface Parameters** page to define the IP addresses on which RIP is enabled, define routing metrics, enable Auto Send, define virtual distance, and define the IP status.

NOTE: To define an RIP interface, RIP must be enabled. See "Enabling RIP, Redistribution of OSPF Routes, Redistribution of Static Routes" for more information.

To open the **RIP Interface Parameters** page, click **Router→RIP→RIP Interface Parameters** in the tree view.

Figure 8-9. RIP Interface Parameters Page



RIP Interface — The current interface IP address.

RIP Version — The type of RIP being broadcast. Possible values are:

Ver. 1 — Broadcasts RIP updates compliant with RFC 1058.

Ver. 2 — Indicates the device is broadcasting RIP 2 updates.

RIP Mode — The type of RIP operation. Possible values are:

RX — RIP receive broadcasts are received on the device.

RX & TX — RIP receive and transmit broadcasts are received on the device.

Auto Send — Enables the device to advertise RIP messages in the default metric only, allowing stations to learn the default router address. As a result, the router is prevented from sending excessive RIP updates on links where no routers exist to receive them. While **Auto Send** is active, a short-form RIP update is sent, which allows stations listening for RIP to do router discovery etc. and to send an RIP update to routers that might be added to the network later.

If a RIP update is received on an interface, **Auto Send** is disabled on that interface, and full RIP updates are sent. If the device detects another RIP message, **Auto Send** is disabled.

Default Route Metric (1-16) — The default route entry metric in RIP updates originating on this interface. Zero indicates that no default route is originated.

Virtual Distance (1-16)— Virtual number of hops assigned to the interface. This fine-tunes the RIP routing algorithm.

Authentication Mode — The interface authentication type, Password or MD5, used to authenticate RIP ver. 2 messages.

Authentication Password — The authentication password.

Authentication Key-Chain — The authentication key chain.

Remove — When checked, removes the RIP interface.

Adding a RIP Interface

1. Open the **RIP Interface Parameters** page.
2. Click **Add** to display the **New RIP Interface** page.
3. Complete the fields on the page.

   The fields on this page are the same as those on the **RIP Interface Parameters** page.
4. Click **Apply Changes**.

Modifying RIP Interface Parameters

1. Open the **RIP Interface Parameters** page.
2. Modify the fields as desired.
3. Click **Apply Changes**.

   The RIP interface parameters are modified, and the device is updated.

Deleting a RIP Interface

1. Open the **RIP Interface Parameters** page.
2. Use the **RIP Interface** drop-down menu to select an RIP interface.
3. Check the **Remove** check box.
4. Click **Apply Changes**.

   The RIP interface is removed and the device is updated.

Configuring RIP Interfaces Using CLI Commands

The following table contains the CLI commands for configuring the RIP Global Parameters.

Table 8-7. RIP Configuration CLI Commands

CLI Command	Description
`rip`	Enables RIP on an interface.
`rip version {1 | 2}`	Specifies an RIP version.
`rip passive-interface`	Disables the sending of routing updates on an interface.
`rip auto-send`	Automatically detects if RIP information is required to be sent on the interface.
`rip offset` *`offset`*	Adds an offset to a metric learned via RIP before adding it to the interface table.
`rip default-route offset` *`offset`*	Generates a default route into RIP by applying an offset value.
`rip authentication {text` *`text | md5 name-of-chain`*`}`	Enables authentication for RIP Version 2 packets and specifies the authentication type.
`show ip rip`	Displays IP RIP information
`show ip rip md5`	Displays IP RIP MD5 information.

The following is an example of the CLI commands:

```
Console (config)# router rip enable
Console(config)# interface ip 100.1.1.1
Console(config-ip)# rip
Console(config-ip)# rip version 1
Console(config-ip)# rip passive interface
Console(config-ip)# rip auto-send
Console(config-ip)# rip offset 5
Console(config-ip)# rip default-route offset 5
Console(config-ip)# rip authorization text dell
Console(config-ip)# exit
Console(config)# exit
```

```
Console# show ip rip
RIP is enabled.
OSPF leaking is enabled.
Static leaking is enabled.
Interface State Ver Offset Default Route Passive Auto Send Auth
176.16.0.0/16   Enabled  21 Disabled               No Yes  MD5
192.168.0.0/16  Enabled 21 Disabled                  No No  Text
```

Configuring OSPF Parameters and Filters

The Open Shortest Path First (OSPF) internal gateway protocol enables routers to exchange link state messages by gathering network information and determining the best routing path based on node distance.

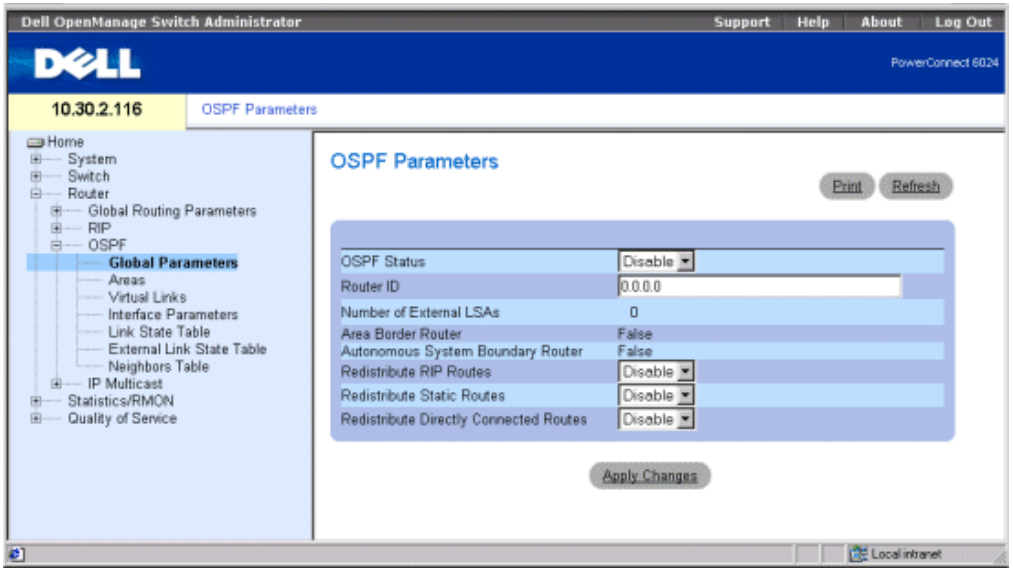
OSPF is a link state protocol rather than a distance vector protocol and, therefore, needs less bandwidth than RIP. OSPF is enabled and defined by:

- Configuring OSPF Parameters
- Configuring OSPF Areas
- Configuring the OSPF Virtual Links
- Viewing the Link State Table
- Viewing the External Link State Table
- Viewing the OSPF Neighbor Table

Configuring OSPF Parameters

OSPF discovers the best routing path based on node distance. OSPF is enabled on the **OSPF Parameters** page. To open the **OSPF Parameters** page, click **Router→OSPF→Global Parameters** in the tree view.

Figure 8-10. OSPF Global Parameters Page



OSPF Status — Enables OSPF on at least one interface, or disables OSPF for all interfaces.

Router ID — The router ID number. By default, the router ID is an IP address on the device. **Router ID** is an optional field, with a default value of the smallest device IP interface.

Number of External LSAs — The number of external link-state advertisements (LSA) in the link-state database.

Area Border Router (ABR) — Indicates whether the device is an area border router. If the device is configured as an ABR, the device is connected to two or more areas. One area is the backbone area.

Autonomous System Boundary Router (ASBR) — Indicates whether the device is configured as an ASBR. If the device is configured as a ASBR, the device imports routing data from non-OSPF routing protocols.

Redistribute RIP Routes — Enables or disables the redistribution of routes inserted into the IP routing table by the RIP protocol to advertise OSPF as external routes.

Redistribute Static Routes — Enables all statically configured routes to be advertised as OSPF external routes or disables redistribution of static routes.

Redistribute Directly Connected Routes — Enables all external routes to advertise to OSPF as external routes or disables redistribution of external direct routes.

Enabling OSPF

1. Open the **OSPF Parameters** page.
2. Define the **OSPF Status**, **Router ID**, **Redistribute RIP Routes**, **Redistribute Static Routes**, and **Redistribute Directly Connected Routes** fields.
3. Click **Apply Changes**.

   OSPF is enabled on the device.

NOTE: OSPF processes can only be cleared using CLI command **clear ip ospf process**.

Enabling OSPF Using CLI Commands

The following table contains the CLI commands for enabling OSPF.

Table 8-8. OSPF CLI Commands

CLI Command	Description
`router ospf enable`	Enables the OSPF routing process.
`router ospf router-id` *`ip-address`*	Configures an OSPF router ID.
`router ospf redistribute rip`	Enables advertising routes, that are learned by the RIP process, in the OSPF routing process.
`router ospf redistribute static`	Advertising routes, configured statically, in the OSPF routing process.
`outer ospf redistribute connected`	Advertising routes directly connected.

The following is an example of the CLI commands:

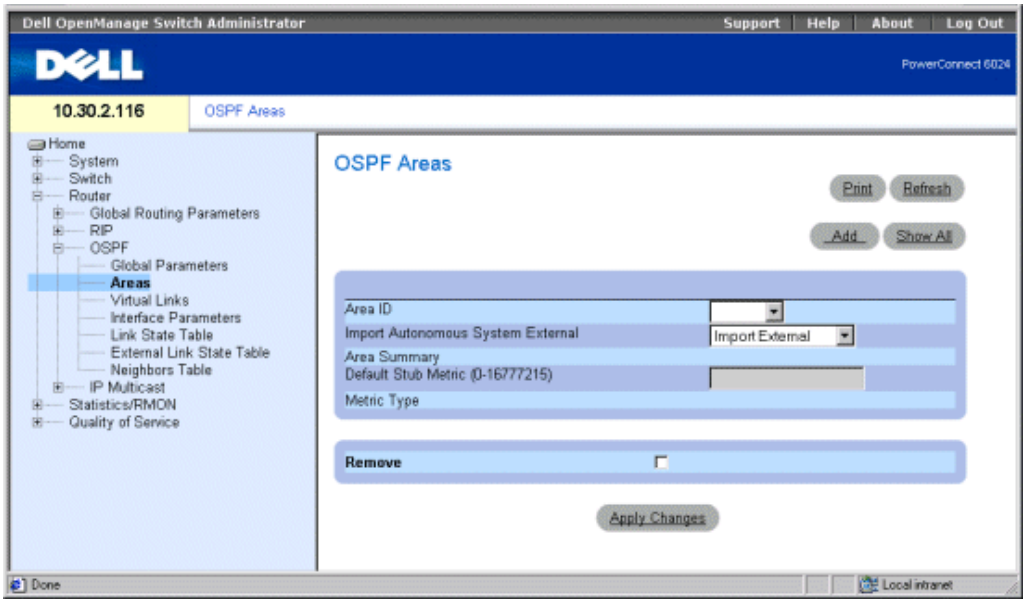
```
Console (config)# router ospf enable
Console (config)# router ospf router-id 196.127.2.1
Console (config)# router ospf redistribute rip
Console (config)# router ospf redistribute static
```

Configuring OSPF Areas

The **OSPF Areas** page contains information for defining and maintaining OSPF areas within which interfaces and virtual links are defined. Once an OSPF area is created, OSPF is automatically enabled on all IP interfaces.

To display the **OSPF Areas** page, click **Router→OSPF→Areas** in the tree view.

Figure 8-11. OSPF Areas Page



Area ID — The area ID. The format is an IP address.

Import Autonamous System External — Indicates whether this is a stub area. Possible values are:

Import External — Autonomous system external link state advertisements (LSA) can be imported into the area

Import No External — External LSAs cannot be imported into the area; therefore, this is a stub area.

Area Summary — Controls the import of summary LSAs into stub areas. This variable has no effect on other areas. Possible values are:

No Area Summary — Specifies that this is a totally stubby area.

Send Area Summary — Specifies that this is not a totally stubby area.

A stub area is an area into which AS External LSAs are not flooded. Totally stubby areas use a default route to reach not only destinations external to the autonomous system, but also all destinations external to the area. To take advantage of the OSPF stub area support, default routing must be used in the stub area.

Default Stub Metric (0-16777216) — The metric of the default route created for the stub area. Stub areas do not import external AS. Therefore, a default route is created by the area border router for the stub area.

Metric Type — The protocol metric type.

Remove — When checked, removes the IP address from the OSPF area table.

Defining a New OSPF Area

1. Open the **OSPF Areas** page.
2. Click **Add** to display the **Add an OSPF Area** page.
3. Complete the fields in the dialog.

NOTE: The **Stub Metric** field is defined for Area Border routers.

4. Click **Apply Changes**.

   The new area is added to the OSPF area table.

Modifying OSPF Area Parameters

1. Open the **OSPF Areas** page.
2. Select an **Area ID**.

   The parameters for the OSPF area display.
3. Modify the fields as desired.
4. Click **Apply Changes**.

   The area parameters are modified and saved to the device.

Deleting an OSPF Area

1. Open the **OSPF Areas** page.
2. Click **Show All** to display the OSPF Area table.
3. Select an OSPF area and check the **Remove** check box.
4. Click **Apply Changes**.

   The OSPF area is removed from the table, and the device is updated.

Defining OSPF Areas Using CLI Commands

The following table contains the CLI commands for defining OSPF areas.

Table 8-9. OSPF Area CLI Commands

CLI Command	Description
`router ospf area` *`area-id`* `stub`	Defines an area as a stub area. To disable this function, use the **no** form of this command.
`router ospf area` *`area-id default-cost cost`*	Specifies a cost for the default summary route sent into a stub area.

The following is an example of the CLI commands:

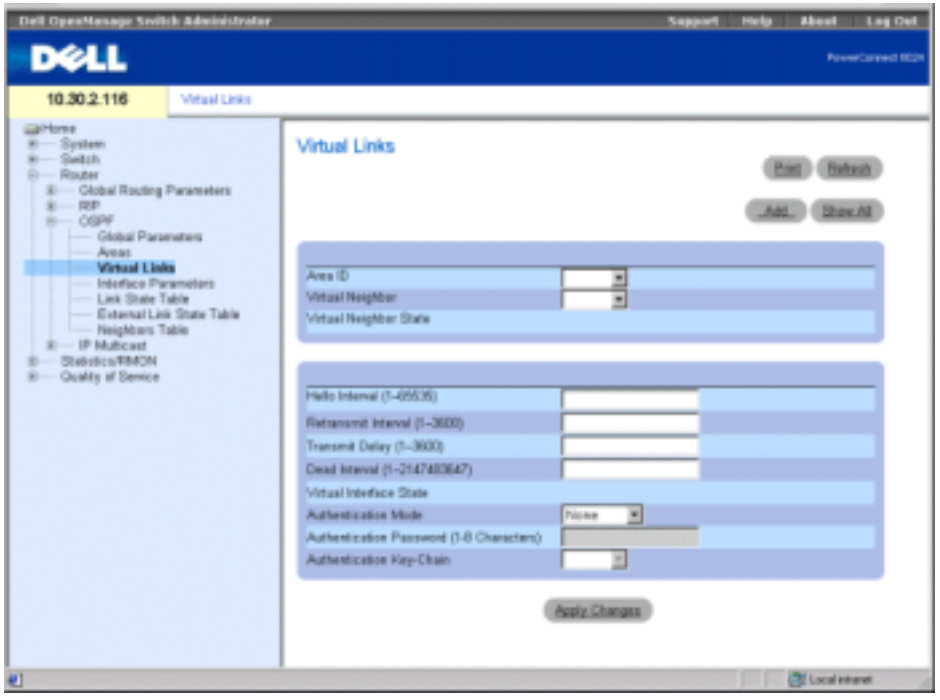
```
Console (config)# router ospf enable
Console (config)# router ospf area 7.7.7.7 stub
Console (config)# router ospf area 192.168.3.1 default-cost 10000
```

Configuring the OSPF Virtual Links

OSPF requires all areas to be linked through a backbone area. However, if an area is not connected to a backbone, you can connect two area border routers through a virtual link. Virtual links are defined by configuring a virtual neighbor. Virtual links cannot be configured through a stub area.

Define virtual links on the **Virtual Links** page. To display the **Virtual Links** page, click **Router→ OSPF→Virtual Links** in the tree view.

Figure 8-12. Virtual Links Page



Area ID — The OSPF interface area ID of the transit area.

Virtual Neighbor — Router ID of the virtual neighbor.

Virtual Neighbor State — State of the virtual neighbor.

Hello Interval (1-65535) — Time (seconds) between Hello packets. All devices attached to a common network must have the same Hello interval. The default is 10 seconds.

Retransmit Interval (0-3600) — Time (seconds) between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds.

Transmit Delay(0-3600) — Estimated time (seconds) required to send a link-state update packet on the interface. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.

Dead Interval (0-2147483647) — Time (seconds) router Hello packets have not been detected, and the router times out. The value must be a multiple of the **Hello Interval** value. All routers attached to a common network must have a value specified for this parameter. The default is 60 seconds.

Virtual Interface State — Indicates the state of the virtual interface.

Authentication Mode — The interface authentication type, Password or MD5, used to authenticate OSPF link state messages.

Authentication Password (1-8 Characters) — The password (eight characters or less) used to authenticate OSPF link sate messages.

Authentication Key-Chain — The MD5 key chain used to authenticate OSPF link sate messages.

Adding a Virtual Link

1. Open the **Virtual Links** page.
2. Click **Add** to display the **Add a Virtual Link** page.

Figure 8-13. Add a Virtual Link Page

3 Define the fields in the page.

4 Click **Apply Changes**.

The new OSPF virtual link is added.

Modifying Virtual Links

1 Open the **Virtual Links** page.

2 Select an area ID from the **Area ID** drop-down menu.

The field parameters display.

3 Modify the desired fields.

4 Click **Apply Changes**.

The OSPF virtual link parameters are modified and saved to the device.

Deleting an OSPF Virtual Link

1 Open the **Virtual Links** page.

2 Click **Show All** to display the **Virtual Links Table**.

3 Select an virtual link.

The field parameters for the table entry display.

4 Check the **Remove** check box.

5 Click **Apply Changes**.

The virtual link is removed, and the device is updated.

Viewing OSPF Virtual Links Using CLI Commands

The following table contains the CLI commands for defining OSPF areas.

Table 8-10. OSPF Virtual Link CLI Commands

CLI Command	Description
`show ip ospf virtual-links [area area-id] [router router-id]`	Displays the parameters and current state of OSPF virtual links.
`router ospf area area-id virtual-link router-id`	Adds a virtual link.

The following is an example of the CLI commands:

```
Console (config)# show ip ospf virtual-links

Virtual Link to router 192.168.101.2 is up

Virtual link has simple password authentication

Transit area 0.0.0.1

Transmit Delay is 1 sec, State POINT_TO_POINT

Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Adjacency State FULL

Console (config)#router ospf area 176.16.1.0 virtual-link
176.16.8.7

Console (config)#router ospf area 176.16.1.0 virtual-link
176.16.8.7
```

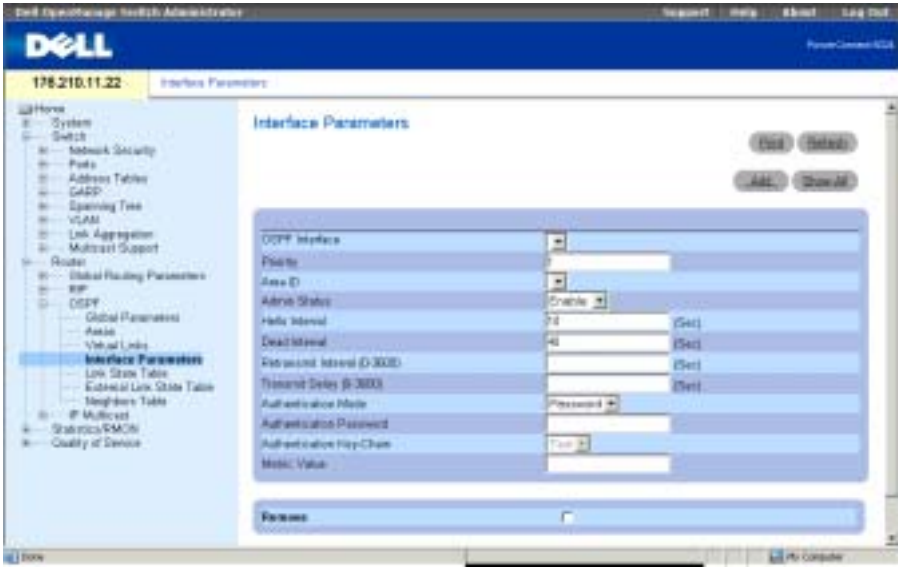
Configuring OSPF Interface Parameters

After OSPF global parameters and areas are defined, you can configure OSPF on each interface.

Auto-creation allows OSPF to be configured automatically on each interface after an area is defined. OSPF interfaces can also be user-defined. The OSPF Interface table enables IP routing using OSPF specific information.

To display the **Interface Parameters** page, click **Router→OSPF→Interface Parameters** in the tree view.

Figure 8-14. Interface Parameters Page



OSPF Interface — IP address of the OSPF interface.

Priority — The interface priority. Value 0 indicates that the device cannot be defined as the designated device on the current network. If more than one device has the same priority, the router ID is used. The possible field value range is 0-255. The default is 1.

Area ID — The OSPF interface area ID.

Admin Status — Enables or disables the OSPF process.

Hello Interval — Time interval in seconds between Hello packets. All devices attached to a common network must have the same Hello interval. The possible field value range is 1-65535. The default is 10 seconds.

Dead Interval — Time interval in seconds before the router times out after Hello packets have not been detected. The value must be a multiple of the **Hello Interval** value. All routers attached to a common network must have a value specified for this parameter. The possible field value range is 1-2147483647. The default is four times the **Hello Interval** value.

Retransmit Interval (0-3600) — Time interval in seconds between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The value must be greater than the expected round-trip delay between any two routers on the attached network. The default is 5 seconds.

Transmit Delay (0-3600) — Estimated amount of time in seconds required to send a link-state update packet on the interface. LSAs in the update packet have their age incremented by this amount before transmission. The default value is 1 second.

Authentication Mode — The interface authentication type, Password or MD5, used to authenticate OSPF link state messages.

Authentication Password — Password used to authenticate OSPF link sate messages. The maximum password length is eight characters.

Authentication Key-Chain — The MD5 key chain used to authenticate OSPF link sate messages.

Metric Value — The metric for this type of service on the interface. The possible field value range is 1-65535.

Remove — When checked, removes an OSPF interface.

Adding an OSPF Interface

1. Open the **Interface Parameters** page.
2. Click **Add** to display the **Add OSPF Interface** page.

Figure 8-15. Add OSPF Interface

3. Complete the fields on the page.
4. Click **Apply Changes**.

   The new OSPF interface is added to the device.

Modifying OSPF Parameters

1. Open the **Interface Parameters** page.
2. Select an OSPF interface to display the field parameters for the table entry.
3. Modify the desired parameters.
4. Click **Apply Changes**.

   The OSPF interface parameters are modified and saved to the device.

Removing an OSPF Interface

1. Open the **Interface Parameters** page.
2. Click **Show All** to display the **OSPF Interface Table**.
3. Select an OSPF interface.
4. Check the **Remove** check box.
5. Click **Apply Changes**.

   The OSPF interface is removed.

Defining OSPF Interfaces Using UCLI Commands

The following table contains the CLI commands for defining OSPF interfaces.

Table 8-11. OSPF Interface CLI Commands

CLI Command	Description
`ospf`	Creates an OSPF routing process on an interface.
`ospf area` *`area-id`*	Defines an interface area ID.
`ospf enable`	Activates OSPF on an interface.
`ospf priority` *`number-value`*	Sets the router priority, which is used in electing the designated router for the network.
`ospf hello-interval` *`seconds`*	Specifies the time interval between hello packets the software sends on an interface.
`ospf dead-interval` *`seconds`*	Sets the time interval during which hello packets must not be sent before neighbors declare the router down.
`ospf retransmit-interval` *`seconds`*	Specifies the time interval between link-state advertisement (LSA) retransmissions for interface adjacencies belonging to the interface.

Table 8-11. OSPF Interface CLI Commands

CLI Command	Description
`ospf transmit-delay` *seconds*	Sets the estimated time required to send a link-state update packet on an interface.
`ospf authentication {text` *text* `| md5` *name-of-chain*`}`	Enables authentication for OSPF packets and specifies the authentication type.
`clear ip ospf process [`*interface*`]`	Clears redistribution based on OSPF routing.
`show ip ospf interface [`*interface*`]`	Displays OSPF-related interface information.

The following is an example of the CLI commands:

```
Console(config)# interface ip 1.100.100.100
Console(config-ip)# ospf
Console(config-ip)# ospf area 192.168.2.1
Console(config-ip)# ospf enable
Console(config-ip)# ospf priority 100
Console(config-ip)# ospf hello-interval 100
Console(config-ip)# ospf dead-interval 100
Console(config-ip)# ospf retransmit-interval 60
Console(config-if)# ospf retransmit-delay 60
Console(config-ip)# ospf authentication text abab
Console(config-ip)# ospf authentication md5 mychain
Console(config-ip)# exit
Console(config)# exit
Console# clear ip ospf process 192.168.3.1
Console# exit
Console# show ip ospf interface 192.168.1.1
IP interface 192.168.1.1/16 is up, OSPF is enabled
Area 0.0.0.0, Router ID 192.77.99.1, Network Type BROADCAST, Cost:
10
Interface has simple password authentication
```

```
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.1.11, Interface address 192.168.1.11
Backup Designated router id 192.168.1.28, Interface addr
192.168.1.28
Timer intervals configured, Hello 10, Dead 60, Retransmit 5
Neighbor Count is 8, Adjacent neighbor count is 2
Adjacent with neighbor 192.168.1.28 (Backup Designated Router)
```

Viewing the Link State Table

The **OSPF Link State Table** page contains link state advertisement information for areas to which the device is attached. Click **Router→OSPF→Link State Table** in the tree view.

Figure 8-16. OSPF Link State Table

Area ID — The area ID.

Link Type — Indicates the link type for the area.

Link ID — The routing domain piece described by the advertisement. It is either a router ID or an IP address.

Router ID — The originating router in the autonomous system.

Sequence Number — The link sequence number. The sequence number detects both old and duplicate links state advertisements. The larger the sequence number the more recent the advertisement.

Age—Indicates the link age state advertisement in seconds.

Checksum—Checksum of the advertisement complete contents, excluding the **Age** value.

Viewing the OSPF Link State Table Using CLI Commands

The following table contains the CLI commands for viewing the OSPF Link State Table.

Table 8-12. OSPF Link State CLI Commands

CLI Command	Description
`show ip OSPF [area-id] database`	Displays information lists related to the OSPF database for a specific router.

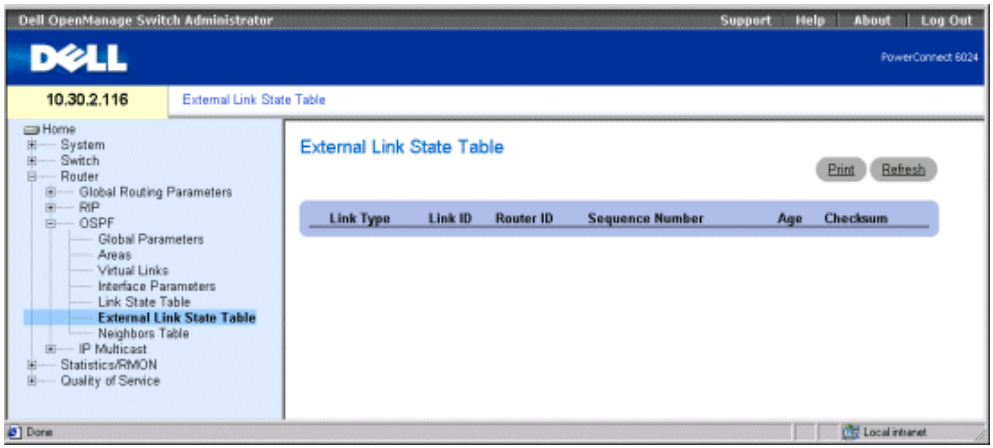
The following is an example of the CLI commands:

```
console> show ip ospf database

OSPF Router with ID 200.1.1.11

Router Link States(Area 0)

Link IDADV RouterAgeSeq#ChecksumLink count

200.1.1.8200.1.1.813810x8000010D0xEF602

200.1.1.11200.1.1.1114600x800002FE0xEB3D4

200.1.1.12200.1.1.1220270x800000900x875D3

200.1.1.27200.1.1.2713230x800001D60x12CC3


Net Link States(Area 0)

Link IDADV RouterAgeSeq#Checksum

140.1.1.27200.1.1.2713230x8000005B0xA8EE

141.1.1.11200.1.1.1114610x8000005B0x7AC
```

Viewing the External Link State Table

The External Link State table contains external link state advertisement information. External Link State table information is learned from sources other than OSPF routes. To display the External Link State table page, click **Router→OSPF→External Link State Table** in the tree view.

Figure 8-17. External Link State Table



Link Type — The external link type. Each link state advertisement has a specific format. This field is always external link.

Link ID — The routing domain piece described by the advertisement. It is either a router ID or an IP address.

Router ID — The originating router in the autonomous system.

Sequence Number — The external link sequence number. The sequence number detects both old and duplicate links state advertisements. The larger the sequence number the more recent the advertisement.

Age — The external link age state advertisement in seconds.

Checksum — Checksum of the advertisement complete contents, excluding the **Age** value.

Viewing the OSPF External Route Table Using CLI Commands

The following table contains the CLI commands for viewing the OSPF External Route Table.

Table 8-13. OSPF External Route Table CLI Commands

CLI Command	Description
`show ip OSPF [area-id] database [external] [link-state-id]`	Lists related to the OSPF database for a specific router.

The following is an example of the CLI commands:

```
Console> show ip ospf database
```

Viewing the OSPF Neighbor Table

The OSPF Neighbor Table describes all neighbors in the subject router's locality. To open the **Neighbor Table** page, click **Router→OSPF→Neighbors Table** in the tree view.

Figure 8-18. Neighbors Table

IP Address — The IP Address this neighbor is using in its IP source address.

Network Mask — The neighboring interface network mask.

Neighbor Selection — Specifies which of the device's neighbor information to display.

Neighbor's Address — The neighbor IP address.

Priority — The neighbor priority.

Router ID — The neighbor Router ID.

State — The neighbor current state.

Displaying the Neighbors List

1. Open the **OSPF Neighbors Table** page.
2. In the **Neighbor Selection** column, click the option button of the neighbor for which you want to view information.
3. Click **Show Neighbor's Info**.

   The neighbor's information displays at the bottom of the page.

Displaying the All Neighbors Table

1. Open the **Neighbors Table** page.
2. Click **Show All** to display the **All Neighbors Table**.

Viewing the OSPF Neighbor Information Using CLI Commands

The following table contains the CLI commands for viewing the OSPF Neighbor Information Table.

Table 8-14. OSPF Neighbor CLI Commands

CLI Command	Description
`show ip ospf neighbor [interface]`	Displays OSPF-neighbor information about a per-interface basis.

The following is an example of the CLI commands:

```
Console> show ip ospf neighbor
ID         Pri State Address  IP interface
-------------------------------------------------
192.168.1.11 1 FULL /DR        192.168.1.11192.168.1.1
192.168.1.12 2 FULL /DROTHER   192.168.1.12192.168.1.1
192.168.2.11 1 FULL /DR        192.168.2.11192.168.2.1
192.168.2.12 2 FULL /DROTHER   192.168.2.12192.168.2.1
Console> show ip ospf neighbor 192.168.1.1
Neighbor 192.168.1.11, Address 192.168.1.11
In the area 0.0.0.0
Neighbor priority is 1, State is FULL
Options 2
Neighbor 192.168.1.12, Address 192.168.1.12
In the area 0.0.0.0
Neighbor priority is 2, State is FULL
Options 2
```

Configuring IP Multicast Routing

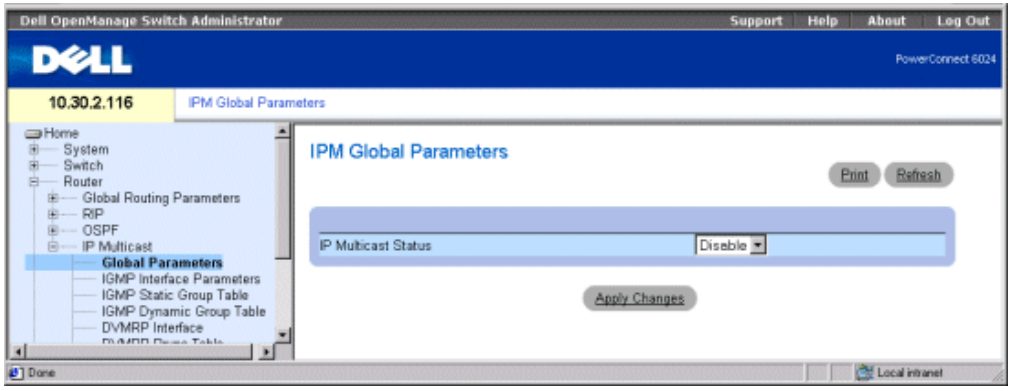
Multicast routing maximizes network resources. One host sends data to a group of hosts (rather than a single host) within the IP network, using the IP multicast group address. IP Multicast routing is implemented in the PowerConnect 6024/6024F using the following protocols:

- Internet Group Member Protocol (IGMP) - Provides a method for discovering which clients are interested in receiving specific transmissions.
- Distance Vector Multicast Routing Protocol (DVMRP) - Allows routers to establish a transmission tree, and copy packets across the transmission routing tree.

Defining IPM Global Parameters

IP Multicast routing is enabled on the **IPM Global Parameters** page. To display the **IPM Global Parameters** page, click **Router→IP Multicast→Global Parameters** in the tree view.

Figure 8-19. IPM Global Parameters



IP Multicast Status — Enables or disables IPM routing on the device.

Enabling IPM Routing on the Device

1. Open the **IPM Global Parameters** page.
2. Select **Enable** in the **IPM Multicast Status** field.
3. Click **Apply Changes**.

   IP Multicast routing is enabled on the device.

Enabling Multicast Routing Using CLI Commands

The following table contains the CLI commands for enabling Multicast routing.

Table 8-15. Multicast Routing CLI Commands

CLI Command	Description
`ip multicast-routing`	Enables IP multicast routing.

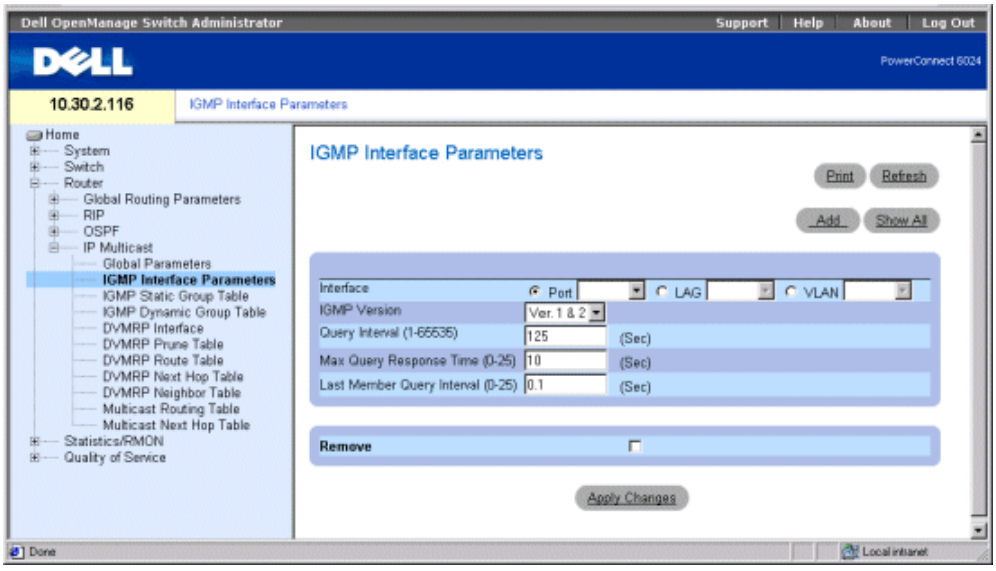
The following is an example of the CLI commands:

```
Console (config)# ip multicast-routing
```

Defining IGMP Interface Parameters

Internet Group Membership Protocol (IGMP) establishes host memberships within a multicast group. IGMP allows hosts to notify routers that they can receive multicast packets addressed to specific multicast groups. To open the **IGMP Interface Parameters** page, click **Router→IP Multicast→IGMP Interface Parameters** in the tree view.

Figure 8-20. IGMP Interface Parameters



Interface — Contains a list of IP addresseses of interfaces for which IGMP has been enabled.

IGMP Version — The current software version of IGMP. The default value is Ver. 1&2.

Query Interval (1-65535) — Amount of time in seconds that query messages are transmitted. You can adjust the amount of IGMP messages sent on sub-networks by adjusting the value of the Query Interval. The larger the value, the less often IGMP messages are sent. The default value is 125 seconds.

Max Query Response Time (0-25) — Maximum response time for advertising IGMP queries. Response time adjusts the amount of traffic on a per sub-network basis. Varying the response time affects the burst of network traffic. The higher the value the longer period of time passes between host responses. The default value is 10 seconds.

Last Member Query Interval (0-25)—Modifies the leave latency of the network. A reduced value reduces the amount of time needed to detect the loss of the last group member. The default value is 0.1.

Remove — When checked, removes the IGMP interface.

Adding an IGMP Interface

1. Open the **IGMP Interface Parameters** page.
2. Click **Add** to display the **Add an IGMP Interface** page.
3. Select an interface from the **New Interface** drop down menu.
4. Complete the fields on the page.
5. Click **Apply Changes**.

   The new IGMP Interface is added to the device.

Modifying an IGMP Interface

1. Open the **IGMP Interface Parameters** page.
2. Select the interface that you want to modify.
3. Modify the desired fields.
4. Click **Apply Changes**.

   The IGMP Interface parameters are modified and saved to the device.

Deleting an IGMP Interface

1. Open the **IGMP Interface Parameters** page.
2. Click **Show All** to display the **IGMP Interface Table** page.
3. Select an IGMP interface, and check the **Remove** check box.
4. Click **Apply Changes**.

   The IGMP interface is removed.

Configuring IGMP Interface Parameters Using CLI Commands

The following table contains the CLI commands for configuring IGMP interface parameters.

Table 8-16. IGMP Interface Parameters CLI Commands

CLI Command	Description
`ip igmp`	Creates IGMP on an interface.
`ip igmp query-interval` *`seconds`*	Configures the frequency at which the software sends IGMP host query messages.
`ip igmp query-max-response-time` *`seconds`* [*`tenths-of-seconds`*]	Configures the maximum response time advertised in IGMP queries.
`ip igmp last-member-query-interval` *`seconds`* [*`tenths-of-seconds`*]	Configures the frequency at which the router sends IGMP group-specific host query messages.
`show ip igmp interface` [`ethernet` *`interface-number`* | `vlan` *`vlan-id`* | *`port-channel number`*]	Displays IGMP-related information about an interface.

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g1
Console (config-if)# ip igmp
Console (config-if)# ip igmp query-interval 60
Console (config-if)# ip igmp query-max-response-time 20
Console (config-if)# ip igmp last-member-query-interval 200
Console (config-if)# exit
Console (config)# exit
Console# disable
Console> show ip igmp interface
Interface Version Query Last Max Querier Interval Memberresponserouter
[sec][mSec][Sec]
----------------------------------------
eth g1260100010198.92.37.33
eth g260100010198.92.36.131
```

Defining IGMP Static Interface Groups

The **IGMP Static Group Table** enables static definition of IGMP groups on specific interfaces.

To open the **IGMP Static Group Table** page, click **Router→IP Multicast→IGMP Static Group Table** in the tree view.

Figure 8-21. IGMP Static Group Table

Interface — Specifies the port, VLAN, or LAG to which the specific multicast group is assigned.

IP Multicast Group Address — IP Multicast group address that is assigned to a interface.

New IP Multicast Group Address — The new IP Multicast group address assigned to an interface.

Assigning an Interface to a Multicast Group

1. Open the **IGMP Static Group Table.**
2. Select an interface in the **Interface** field.
3. Select an IP Address in the **Multicast Group Address** field, or define a new multicast group address in the **New Multicast Group Address** field.
4. Click **Apply Changes**.

Displaying the Static Interface Grouping Table

1. Open the **IGMP Static Group Table**.
2. Click **Show All** to display the **Static Interface Grouping Table**.

The page contains the following fields:

- **Interface** — The IP Multicast Group address of which the port is a member.
- **IP Multicast Group** — The IP multicast group to which this interface is a member.
- **Group Up Time** — Indicates in ticks the amount of time that has passed since the entry was created. The time format is hour/minute/second.
- **Last Reporter** — The last member to join the IP Multicast group. If no member has entered the IP Multicast group, the value is 0.0.0.0.
- **Remove** — When checked, removes an IGMP interface.

Configuring Static Interface Grouping Using CLI Commands

The following table contains the CLI commands for static interface grouping.

Table 8-17. Static Interface Grouping CLI Commands

CLI Command	Description
`ip igmp static-group` *`group-address`*	Configures the router to be a statically connected member of the specified group on the interface.

The following is an example of the CLI commands:

```
Console (config)# interface ethernet g5
Console (config-if)# ip igmp static-group 192.168.4.1
```

Viewing the IGMP Dynamic Group Table

The **IGMP Dynamic Group Table** displays IGMP information regarding each IP Multicast group whose members were dynamically assigned to an interface on a physical port.

To open the **IGMP Dynamic Group Table**, click **Router→IP Multicast→IGMP Dynamic Group Table** in the tree view.

Figure 8-22. IGMP Dynamic Group Table

Interface — Specifies an interface belonging to the IP Multicast Group.

Multicast Group Address — The IGMP multicast IP address.

Group Up Time — Indicates in ticks the amount of time that has passed since the entry was created. The time format is hour/minute/second.

Group Expiry Time—Amount of time before the dynamic entry is aged out. The time format is hour/minute/second.

Last Reporter — The last member to join the IP Multicast group. If no member has entered the IP Multicast group the value is 0.0.0.0.

Viewing IGMP Groups Using CLI Commands

The following table contains the CLI commands for viewing the IGMP groups.

Table 8-18. IGMP Group CLI Commands

CLI Command	Description
`show ip igmp groups [group ip-address] [ethernet interface-number | vlan vlan-id | port-channel number]`	Displays the Multicast groups with receivers that are directly connected to the router, and that were learned through Internet Group Membership Protocol (IGMP).

The following is an example of CLI commands:

```
Console> show ip igmp groups
Group Address    Interface Uptime Expires Last Reporter
-------------------------------------------------
 239.255.255.254 eth g11w0d00:02:19    172.21.200.159
224.0.1.40       eth g31w0d00:02:15    172.21.200.1
224.0.1.40       eth g31w0d00:02:1     static
224.0.1.1        eth g11w0d00:02:11    172.21.200.11
224.9.9.2        eth g11w0d00:02:17    172.21.200.155
232.1.1.1        eth g15d21h00:02:11   172.21.200.206
```

Configuring DVMRP Interfaces

Distance Vector Multicast Routing Protocol (DVMRP) uses the Reverse Path Forwarding (RPF) Multicast algorithm to create source based multicast delivery trees. DVMRP is an RPF checking protocol based on DVMRP Routing information. The routing information is collected during routing the exchange.

The **DVMRP Interface** page contains information about DVMRP interface configurations.

To open the **DVMRP Interface** page, click **Router→IP Multicast→DVMRP Interface** in the tree view.

Figure 8-23. DVMRP Interface

The **DVMRP Interface** page contains the following fields divided into two areas:

STATIC ROUTE

Interface — Specifies the interface number on which DVMRP is enabled.

IP Address (X.X.X.X) — Specifies the source IP address of the port on which DVMRP is enabled.

Network Mask (X.X.X.X) — Specifies the subnetwork mask of the source IP address.

Prefix Length /XX) — Specifies the number of bits that comprise the source IP prefix or the network mask of the source IP address.

DVMRP INTERFACE SETTING

IP Interface — Specifies the interface number on which DVMRP is enabled.

IP Address — Indicates the source IP address of the port on which DVMRP is enabled.

DVMRP Metric (1-31) — Indicates the distance used to calculate distance vector. The DVMRP metric is the interface distance between the router originating the report and the source network. The default value is 1.

Remove — When checked, removes a DVMRP interface.

Adding a New DVMRP Interface

1 Open the **DVMRP Interface** page.

2 Click **Add** to display the **Add a DVMRP Interface** page.

3 Define the interface number and DVMRP metric.

4 Click **Apply Changes**.

The DVMRP interface is added to the **IP Interface** list, and the device is updated.

Modifying a DVMRP Interface

1 Open the **DVMRP Interface** page.

2 Select an interface in the **IP Interface** list.

3 Modify the desired fields.

4 Click **Apply Changes**.

The selected DVMRP interface is added to the **DVMRP Interface** list and the device is updated.

Deleting a DVMRP Interface

1 Open the **DVMRP Interface** page.

2 Select an interface in the **IP Interface** list.

3 Check the **Remove** check box.

4 Click **Apply Changes**.

The modified DVMRP interface is deleted from the **IP Interface** list and the device is updated.

Configuring the DVMRP Interfaces Using CLI Commands

The following table contains the CLI commands for configuring and viewing DVMRP interfaces.

Table 8-19. DVMRP CLI Commands

CLI Command	Description
`ip dvmrp`	Enables DVRMP on an interface.
`no ip dvmrp`	Disables DVRMP on an interface.
`ip dvmrp metric` *`metric`*	Configures the interface metric for DVMRP. Metric can be 1-31.
`no ip dvmrp metric`	Disables the interface metric for DVMRP.
`show ip dvmrp interface [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Shows the interface table.

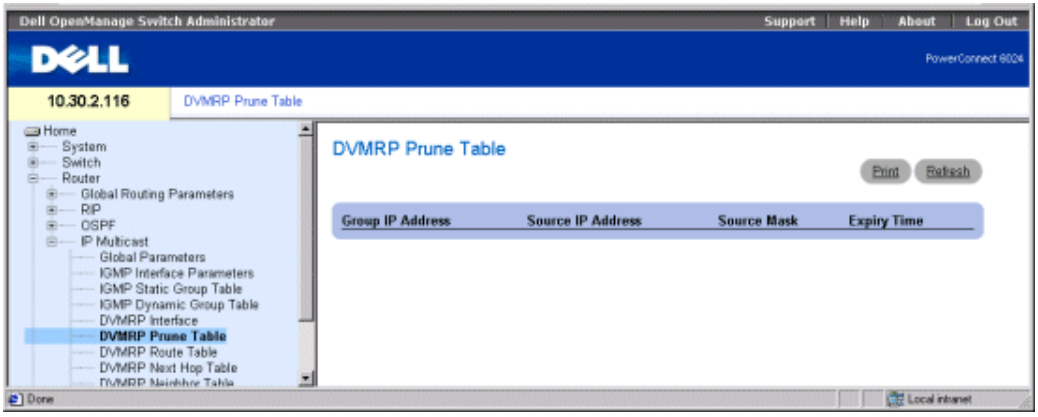
The following is an example of the CLI command:

```
Console (config-if)# interface ethernet g5
Console (config-if)# ip dvmrp
Console (config-if)# ip dvmrp metric 15
Console (config-if)# exit
Console (config)# exit
Console> show ip dvmrp interface
Multicast routing enabled.
Multicast routing protocol is DVMRP.
Interface IP address Metric RCV Bad RCV Bad Sent PacketsRoutesRoutes
-----------------------------------------------
eth g1 172.16.1.1 10012
```

DVMRP Prune Table

The **DVMRP Prune Table** page lists the routers upstream prune state. To open the **DVMRP Prune Table** page, click **Router→IP Multicast→DVMRP Prune Table** in the tree view.

Figure 8-24. DVMRP Prune Table



Group IP Address — IP address of the prune group.

Source IP Address — Source IP address to be pruned.

Source Mask — Source IP mask that has been pruned.

Expiry Time — The remaining time before the upstream flow is pruned.

Viewing the DVMRP Prune Table Using CLI Commands

The following table contains the CLI command for viewing the Prune Table.

Table 8-20. DVRMP Table CLI Commands

CLI Command	Description
`show ip dvmrp prune [group` *`group-address`*`] [`*`source-address`*`]`	Shows the table.

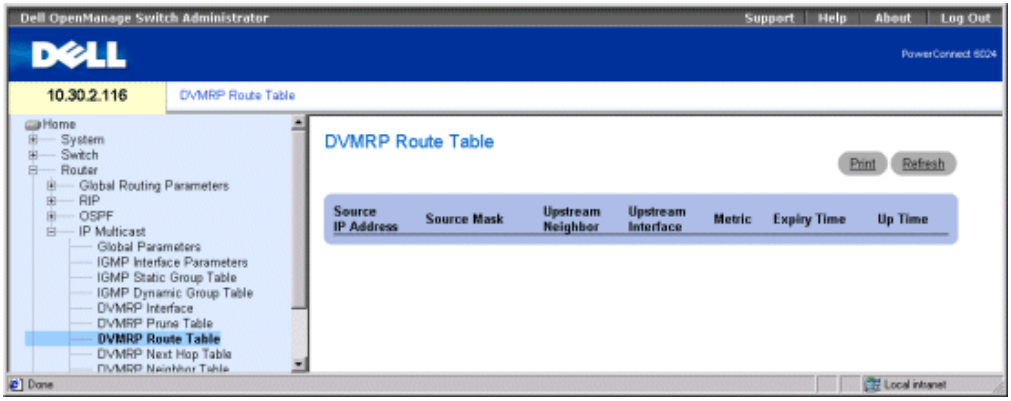
The following is an example of the CLI command:

```
Console> show ip dvmrp prune
Group          Source           Expiry Time
--------------------------------
224.192.78.88 171.68.0.0/16     00:02:52
224.192.78.89 171.68.0.0/16     00:08:52
```

DVMRP Route Table

The **DVMRP Route Table** page contains information about routes learned through DVMRP router exchange. To open the **DVMRP Route Table** page, click **Router→IP Multicast→DVMRP Route Table** in the tree view.

Figure 8-25. DVMRP Route Table



Source IP Address — IP address of the source of the multicast routing information.

Source Mask — Source IP address network mask.

Upstream Neighbor — IP address of the upstream RPF neighbor, from which source IP datagrams are received.

Upstream Interface — The upstream interface IP address.

Metric — Distance in hops to the source subnet.

Expiry Time — Amount of time before the entry is aged out.

Up Time — Amount of time that has passed since the router was learned by the router.

Viewing the DVMRP Route Table Using CLI Commands

The following table contains the CLI command for viewing the DVMRP Route Table.

Table 8-21. DVRMP Route Table CLI Command

CLI Command	Description
`show ip dvmrp route [ip-address] [ip-address]`	Shows the DVMRP route table.

The following is an example of the CLI command:

```
Console> show ip dvmrp route

Source           Neighbor          Interface    Metric    Expiry
Up Time Time

-----------------------------------------------------

171.68.0.0/16   192.168.1.2816  eth g116  11016  100:02:5216  107:55:50
```

DVMRP Next Hop Table

The **DVMRP Next Hop Table** page contains information regarding the outgoing interface's next hop for IP multicast packets. To open the **DVMRP Next Hop Table** page, click **Router→IP Multicast→DVMRP Next Hop Table** in the tree view.

Figure 8-26. DVMRP Next Hop Table

Source IP Address — Source IP address for the next hop of an outgoing interface.

Source Mask — Source mask for the next hop of an outgoing interface.

Downstream Interface — The next hop's outgoing interface.

Type — Specifies the next hop type. Possible values are:

Branch — Indicates that there is another hop after this hop.

Leaf — Indicates that this is the route's last hop.

Viewing the DVMRP Next Hop Table Using CLI Commands

The following table contains the CLI command for viewing the DVMRP Next Hop Table.

Table 8-22. DVMRP Next Hop Table CLI Commands

CLI Command	Description
`show ip dvmrp next-hop [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Shows the DVMRP Next Hop table.

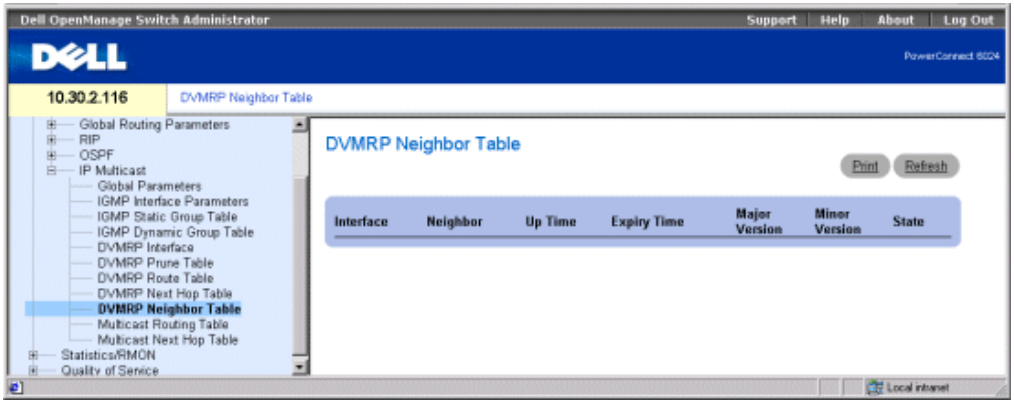
The following is an example of the CLI command:

```
Console> show ip dvmrp next-hop
Source            Interface Hop Type
------------------------- ----------
198.92.37.100/32  eth g2    Leaf
```

DVMRP Neighbor Table

The **DVMRP Neighbor Table** page contains information about neighboring port interfaces. DVMRP neighbors are discovered through DVMRP messages. To open the **DVMRP Neighbor Table** page, click **Router→IP Multicast→DVMRP Neighbor Table** in the tree view.

Figure 8-27. DVMRP Neighbor Table



Interface — Interface number on which DVMRP is enabled.

Neighbor — IP address of the neighboring interface.

Up Time — Amount of time since the neighboring interface became a neighbor.

Expiry Time — Indicates the minimum amount of time before the interface is timed out.

Major Version — The neighboring router's major version number.

Minor Version — The neighboring router's minor version number.

State — The neighboring device state.

Viewing the DVMRP Neighbor Table Using CLI Commands

The following table contains the CLI command for viewing the DVMRP Neighbor Table.

Table 8-23. DVMRP Neighbor Table CLI Commands

CLI Command	Description
`show ip dvmrp neighbor [ethernet` *`interface-number`* `| vlan` *`vlan-id`* `| port-channel` *`number`*`]`	Shows the DVMRP Neighbor table.

The following is an example of the CLI command:

```
Console> show ip dvmrp neighbor ethernet g1
Interface Neighbor Up Expiry Version Capabilities RCV BadState Time      Time    Routes Routes
-----------------------------------------
eth g1 192.168.1.282 0:20:000:02:553.255L,P,G,M110Active
eth g1 192.168.1.102 0:20:000:02:553.255L,P,G,M180Active
eth g2 192.168.1.282 0:20:000:02:553.255L,P,G,M110Active
eth g2 192.168.1.892 0:20:000:02:553.255L,P,G,M180Active
```

Viewing the IP Multicast Routing Table

The **IP Multicast (IPM) Routing Table** contains multicast routing information of IP packets sent from a specific source to IP multicast groups known to the IP Multicast router.

To open the **IP Multicast (IPM) Routing Table**, click **Router→IP Multicast→Multicast Routing Table** in the tree view.

Figure 8-28. IP Multicast (IPM) Routing Table

The **IP Multicast (IPM) Routing Table** contains the following fields:

Multicast Group — IP address of the multicast group.

Source IP — Source IP address of the device to which the multicast information applies.

Source Mask — Masks all or parts of the source IP address.

Upstream Neighbor — IP address of the next upstream device from which packets to the IP address are received.

Upstream Interface — Port number to which multicast packets being sent are received.

Up Time — Indicates the time lapse since the router learned the multicast information.

Protocol — Identifies the type of protocol used to learn the multicast information. For this project, the only possible value is **DVMRP**, which indicates that the Distance Vector Multicast Routing Protocol was used to learn the multicast information.

Displaying IP Multicast Routing Table Using CLI Commands

The following table contains the CLI commands for viewing the IP Multicast Routing Table.

Table 8-24. IP Multicast Routing Table CLI Commands

CLI Command	Description
`show ip mroute [group` *`group-address`*`] [source` *`source-address`*`] [ethernet` *`interface-number`* `|` *`vlan vlan-id`* `|` *`port-channel number`*`]`	Displays the IP multicast routing table contents.

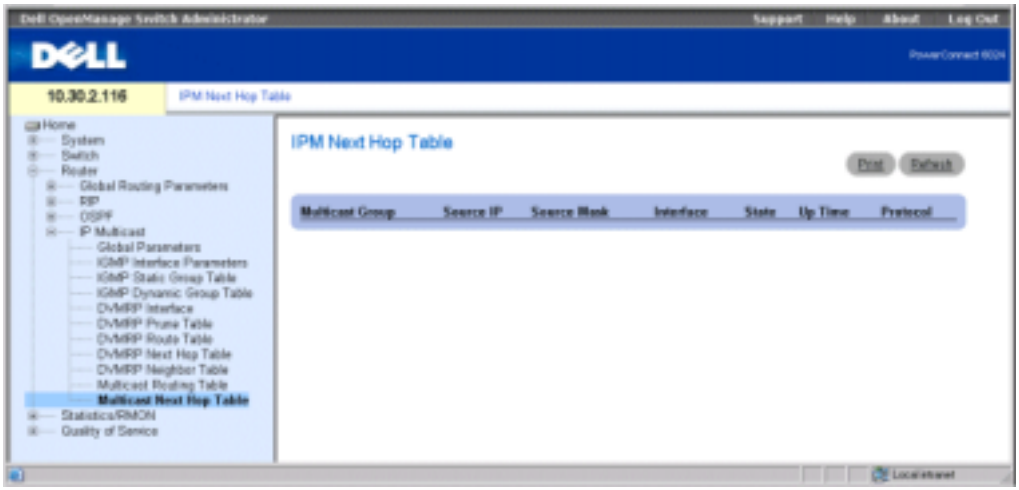
The following is an example of the CLI commands:

```
Console> show ip mroute
Group   Source  Upstream  Interface Up TimeExpiry Time Owner
-----------------------------------------------------
224.0.255.1198.92.37.100/3210.20.37.33 eth g1 20:20:000:02:55dvmrp
224.0.255.1199.92.37.100/3210.20.37.33 eth g1 1d:4h:20m0:02:55dvmrp
224.1.255.1198.92.37.100/3210.20.37.33 eth g1 21:20:000:02:55dvmrp
224.1.255.1199.92.37.100/3210.20.37.33 eth g1 1d:5h:20m0:02:55dvmrp
224.8.255.1179.82.17.200/3210.20.37.33 vlan 127 1w:1d:2h0:02:55dvmrp
224.8.255.1179.82.17.200/3210.20.37.33 vlan 1283m:2w:2d0:02:55dvmrp
224.8.255.1179.82.17.200/3210.20.37.33 vlan 1291y:2m:2w0:02:55dvmrp
224.9.255.1179.82.17.200/3210.20.37.33p-c 71d:5h:20m0:02:55dvmrp
```

Viewing the IP Multicast Next Hop Table

The **IPM Next Hop Table** page contains multicast next hop information. To open the page, click **Router→IP Multicast→Multicast Next Hop Table** in the tree view.

Figure 8-29. IPM Next Hop Table



Multicast Group — IP address of the multicast group.

Source IP — Source IP address of the device to which the multicast information applies.

Source Mask — Masks all or parts of the source IP address.

Interface — Port number to which multicast packets being sent are received.

State — Indicates if the port and next-hop are being used to forward multicast packets. Possible values are:

Pruned — The port and next hop are not being used to forward multicast packets.

Forwarding — The port and the next hop are currently being used to forward multicast packets.

Up Time — The time lapse since the router learned the multicast information.

Protocol — The type of protocol used to learn the multicast information. For this product, the only possible value is **DVMRP**, which indicates that the Distance Vector Multicast Routing Protocol was used to learn the multicast information.

Displaying IPM Next Hop Table Using CLI Commands

The following table contains the CLI commands for viewing the IP Multicast Next Hop table.

Table 8-25. IPM Next Hop CLI Commands

CLI Command	Description
`show ip mroute-next-hop [group` *`group-address`*`] [source` *`source-address`*`]`	Displays the IP multicast next hop table contents.

The following is an example of the CLI commands:

```
Console> show ip mroute-next-hop

Group       Source          Interface Up TimeExpiry TimeStateOwner
-------------------------------------------------------------
224.0.255.1 198.92.37.100/32eth g22  0:20:000:02:55 Forward igmp
224.0.255.1 199.92.37.100/32eth g21  :4d:20m0:02:55 Forward igmp
224.1.255.1 198.92.37.100/32eth g22  1:20:000:02:55 Forward dvmrp
224.1.255.1 199.92.37.100/32eth g21  :4d:20m0:02:55 Forward dvmrp
```

9

Viewing Statistics

This section contains statistics on interface, GVRP, etherlike, RMON, and device utilization.

NOTE: CLI commands are not available for all the Statistics pages.

Viewing Tables

The **Table Views** page contains links for displaying statistics in a chart form.

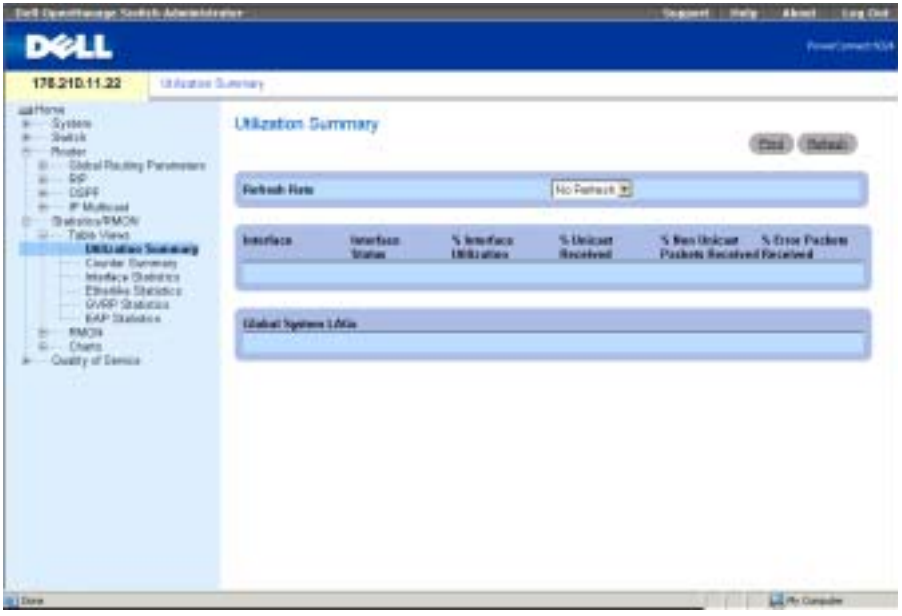
To open the page, click **Statistics/RMON→Table Views** in the tree view.

Viewing Utilization Summary

The **Utilization Summary** page contains statistics for interface utilization.

To open the page, click **Statistics/RMON →Table Views→Utilization Summary** in the tree view.

Figure 9-1. Utilization Summary



The **Utilization Summary** page contains the following fields:

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Interface — The interface number.

Interface Status — Status of the interface.

% Interface Utilization — Network interface utilization percentage based on the duplex mode of the interface. The range of this reading is from 0 to 200 %. The maximum reading of 200% for a full duplex connection indicates that 100% of bandwidth of incoming and outgoing connections is used by the traffic travelling through the interface. The maximum reading for a half duplex connection is 100%.

% Unicast Received — Percentage of Unicast packets received on the interface.

% Non Unicast Packets Received — Percentage of non-Unicast packets received on the interface.

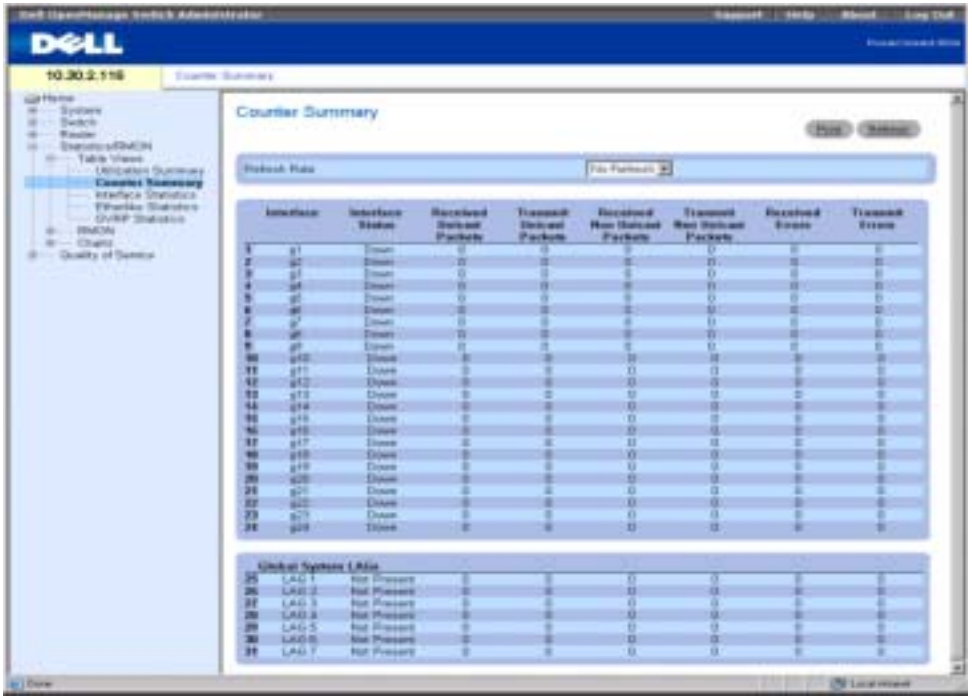
% Error Packets Received — Number packets with errors received on the interface.

Viewing Counter Summary

The **Counter Summary** page contains statistics for port utilization in numeric sums as opposed to percentages.

To open the page, click **Statistics/RMON→Table Views→Counter Summary** in the tree view.

Figure 9-2. Counter Summary Page



Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Interface — The interface number.

Interface Status — Status of the interface.

Received Unicast Packets — Number of received Unicast packets on the interface.

Transmit Unicast Packets — Number of transmitted Unicast packets from the interface.

Received non-Unicast Packets — Number of received non-Unicast packets on the interface.

Transmit non-Unicast Packets — Number of transmitted non-Unicast packets from the interface.

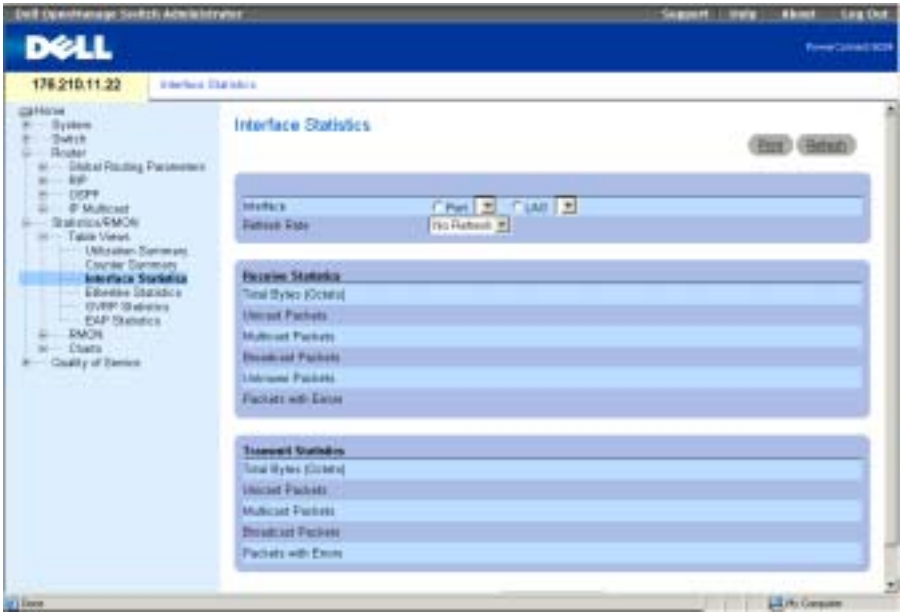
Received Errors—Number of received errors on the interface.

Transmit Errors — Number of transmitted errors from the interface.

Viewing Interface Statistics

The **Interface Statistics** page contains statistics for both received and transmitted packets. The fields for both received and transmitted packets are identical. To open the page, click **Statistics/RMON→Table Views→Interface Statistics** in the tree view.

Figure 9-3. Interface Statistics Page



Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Receive Statistics

Total Bytes (Octets) — Amount of octets received on the selected interface.

Unicast Packets — Amount of Unicast packets received on the selected interface.

Multicast Packets — Amount of Multicast packets received on the selected interface.

Broadcast Packets — Amount of Broadcast packets received on the selected interface.

Unknown Packets — Amount of unknown packets received on the selected interface.

Packets with Errors — Amount of errors transmitted from the selected interface.

Transmit Statistics

Total Bytes (Octets) — Amount of octets transmitted on the selected interface.

Unicast Packets — Amount of Unicast packets transmitted on the selected interface.

Multicast Packets — Amount of Multicast packets transmitted on the selected interface.

Broadcast Packets — Amount of Broadcast packets transmitted on the selected interface.

Packets with Errors — Amount of errors transmitted from the selected interface.

Displaying Interface Statistics

1. Open the **Interface Statistics** page.
2. Select an interface in the **Interface** field.

Resetting Interface Statistics Counters

1. Open the **Interface Statistics** page.
2. Click **Reset All Counters**.

Viewing Interface Statistics Using the CLI Commands

The following table contains the CLI commands for viewing interface statistics.

Table 9-1. Interface Statistics CLI Commands

CLI Command	Description
`show interfaces counters [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays traffic seen by the physical interface.

The following is an example of the CLI commands.

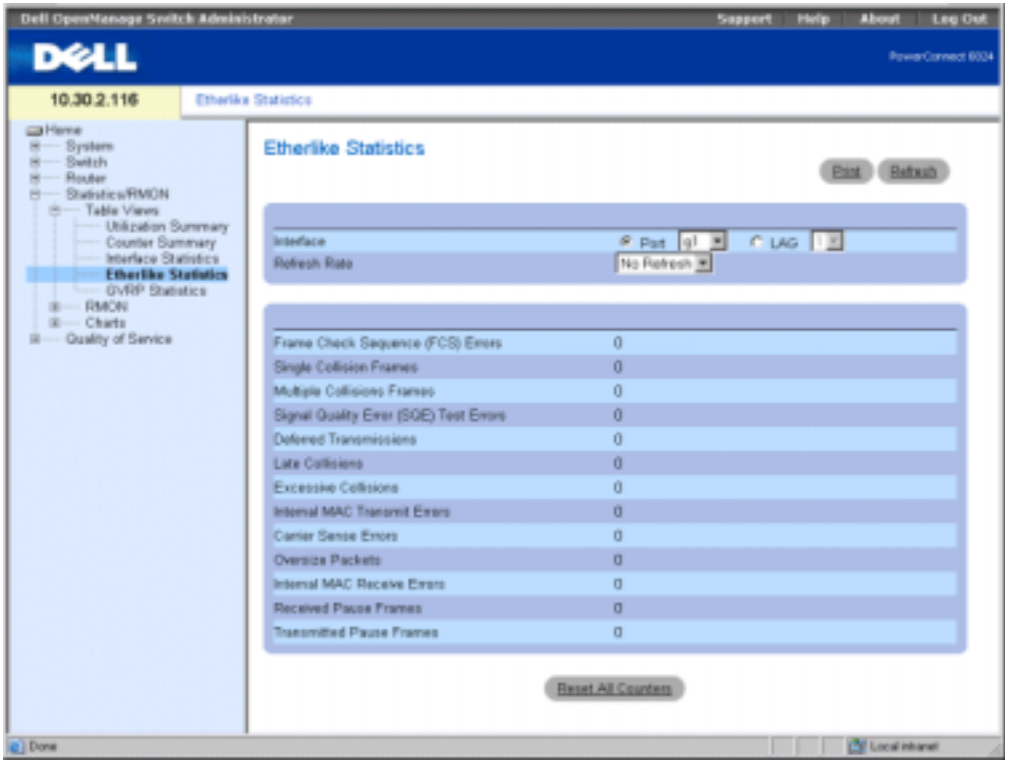
```
Console> show interfaces counters

Port InOctets InUcastPkts InMcastPkts InBcastPkts

-----------------------------------------------

g1   0        0           0           0

g2   0        0           0           0

g3   0        0           0           0

g4   0        0           0           0

g5   0        0           0           0

g6   0        0           0           0

g7   0        0           0           0

g8   0        0           0           0

g9   0        0           0           0

g10  0        0           0           0

g11  0        0           0           0
```

```
g12  10        685          290          32
g13  0         0            0            0
g14  0         0            0            0
g15  0         0            0            0
g16  0         0            0            0
g17  0         0            0            0
g18  0         0            0            0
g19  0         0            0            0
g20  0         0            0            0
g21  0         0            0            0
g22  0         0            0            0
g23  0         0            0            0
g24  0         0            0            0
```

Viewing Etherlike Statistics

The **Etherlike Statistics** page contains interface statistics. To open the page, click **Statistics/RMON→Table Views→Etherlike Statistics** in the tree view.

Figure 9-4. Etherlike Statistics Page



Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Frame Check Sequence (FCS) Errors — Number of FCS errors received the selected interface.

Signal Collision Frames — Number of signal collision frame errors received the selected interface.

Multiple Collision Frames — Number of multiple collisions frame errors received the selected interface.

Single Quality Error (SQE) Test Errors — Number of SQE test errors received on the selected interface.

Deferred Transmissions — Number of deferred transmissions the selected interface.

Late Collisions — Number of late collisions received the selected interface.

Excessive Collisions — Number of excessive collisions received the selected interface.

Internal MAC Transmit Errors — Number of internal MAC transmit errors on the selected interface.

Carrier Sense Errors — Number of carrier sense errors on the selected interface.

Oversize Packets — Number of too-long of packet errors on the selected interface.

Internal MAC Receive Errors — Number of internal MAC received errors on the selected interface.

Receive Pause Frames — Number of received paused errors on the selected interface.

Transmitted Paused Frames — Number of transmitted paused errors on the selected interface.

Displaying Etherlike Statistics for an Interface

1. Open the **Etherlike Statistics** page.
2. Select an interface in the **Interface** field.
3. Click **Query** to display the interface's Etherlike statistics.

Resetting Etherlike Statistics

1. Open the **Etherlike Statistics** page.
2. Click **Reset All Counters**.

Viewing GVRP Statistics

The **GVRP Statistics** page contains device statistics for GVRP. To open the page, click **Statistics/RMON→Table Views→GVRP Statistics** in the tree view.

Figure 9-5. GVRP Statistics Page

Interface — Specifies whether statistics are displayed for a port or LAG.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Join Empty — Device GVRP Join Empty statistics.

Empty — Device GVRP Empty statistics.

Leave Empty — Device GVRP Leave Empty statistics.

Join In — Device GVRP Join In statistics.

Leave In — Device GVRP Leave in statistics.

Leave All — Device GVRP Leave all statistics.

Invalid Protocol ID — Device GVRP Invalid Protocol ID statistics.

Invalid Attribute Type — Device GVRP Invalid Attribute ID statistics.

Invalid Attribute Value — Device GVRP Invalid Attribute Value statistics.

Invalid Attribute Length — Device GVRP Invalid Attribute Length statistics.

Invalid Event — Device GVRP Invalid Event statistics.

Displaying GVRP Statistics for a Port:

1. Open the **GVRP Statistics** page.
2. Select an interface in the **Interface** field.

Resetting GVRP Statistics

1. Open the **GVRP Statistics** page.
2. Click **Reset All Counters**.

Viewing GVRP Statistics Using the CLI Commands

The following table contains the CLI commands for viewing GVRP statistics.

Table 9-2. GVRP Statistics CLI Commands

CLI Command	Description
`show gvrp statistics [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays GVRP statistics.
`show gvrp error-statistics [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays GVRP error statistics.

The following is an example of the CLI commands:

```
Console# show gvrp statistics

GVRP statistics:

----------------

Legend:

rJE  : Join Empty ReceivedrJIn : Join In Received

rEmp : Empty ReceivedrLIn : Leave In Received

rLE  : Leave Empty ReceivedrLA  : Leave All Received
```

```
sJE  : Join Empty SentsJIn : Join In Sent
sEmp : Empty SentsLIn : Leave In Sent
sLE  : Leave Empty SentsLA  : Leave All Sent
Port rJE rJIn rEmp rLIn rLE rLA sJE sJIn sEmp sLIn sLE sLA
---- --- ---- ---- ---- --- --- --- --- --- ---- --- ---
g1   0   0    0    0    0   0   0   0   0   0    0   0
g2   0   0    0    0    0   0   0   0   0   0    0   0
g3   0   0    0    0    0   0   0   0   0   0    0   0
g4   0   0    0    0    0   0   0   0   0   0    0   0
g5   0   0    0    0    0   0   0   0   0   0    0   0
g6   0   0    0    0    0   0   0   0   0   0    0   0
g7   0   0    0    0    0   0   0   0   0   0    0   0
g8   0   0    0    0    0   0   0   0   0   0    0   0
Console# show gvrp error-statistics
GVRP error statistics:
----------------
Legend:
INVPROT : Invalid Protocol IdINVPLEN  : Invalid PDU Length
INVATYP : Invalid Attribute TypeINVALEN  : Invalid Attribute
Length
INVAVAL : Invalid Attribute ValueINVEVENT : Invalid Event

Port INVPROT INVATYP INVAVAL INVPLEN INVALEN INVEVENT
---- ------- ------- ------- ------- ------- -------
g1   0       0       0       0       0       0
g2   0       0       0       0       0       0
g3   0       0       0       0       0       0
g4   0       0       0       0       0       0
g5   0       0       0       0       0       0
g6   0       0       0       0       0       0
g7   0       0       0       0       0       0
g8   0       0       0       0       0       0
```

Viewing EAP Statistics

The **EAP Statistics** page contains information about EAP packets received on a specific port. For more information about EAP, see "Port Based Authentication (802.1x)".

To open the **EAP Statistics** page, click **Statistics/RMON→Table Views→EAP Statistics** in the tree view.

Figure 9-6. EAP Statistics

The **EAP Statistics** page contains the following fields:

Port — The port which is polled for statistics.

Refresh Rate — Amount of time that passes before the interface statistics are refreshed.

Frames Receive — The number of valid EAPOL frames received on the port.

Frames Transmit — The number of EAPOL frames transmitted via the port.

Start Frames Receive — The number of EAPOL Start frames received on the port.

Log off Frames Receive — The number of EAPOL Log off frames that have been received on the port.

Respond ID Frames Receive — The number of EAP Respond ID frames that have been received on the port.

Respond Frames Receive — The number of valid EAP Respond frames received on the port.

Request ID Frames Transmit — The number of EAP Requested ID frames transmitted via the port.

Request Frames Transmit — The number of EAP Request frames transmitted via the port.

Invalid Frames Receive — The number of unrecognized EAPOL frames received on this port.

Length Error Frames Receive — The number of EAPOL frames with an invalid Packet Body Length received on this port.

Last Frame Version — The protocol version number attached to the most recently received EAPOL frame.

Last Frame Source — The source MAC address attached to the most recently received EAPOL frame.

Displaying EAP statistics for a Port

1. Open the **EAP Statistics** page.
2. Select an interface in the **Interface** field.

   The interface EAP statistics are displayed.

Viewing EAP Statistics Using the CLI Commands

The following table summarizes the CLI commands for viewing EAP statistics.

Table 9-3. EAP Statistics CLI Commands

CLI Command	Description
show dot1x statistics ethernet *interface*	Displays 802.1X statistics for the specified interface.

The following is an example of the CLI commands:

```
console# show dot1x statistics ethernet g11
EapolFramesRx: 11
EapolFramesTx: 12
EapolStartFramesRx: 1
EapolLogoffFramesRx: 1
EapolRespIdFramesRx: 3
EapolRespFramesRx: 6
EapolReqIdFramesTx: 3
EapolReqFramesTx: 6
InvalidEapolFramesRx: 0
EapLengthErrorFramesRx: 0
LastEapolFrameVersion: 1
LastEapolFrameSource: 0008.3b79.8787
```

Viewing RMON Statistics

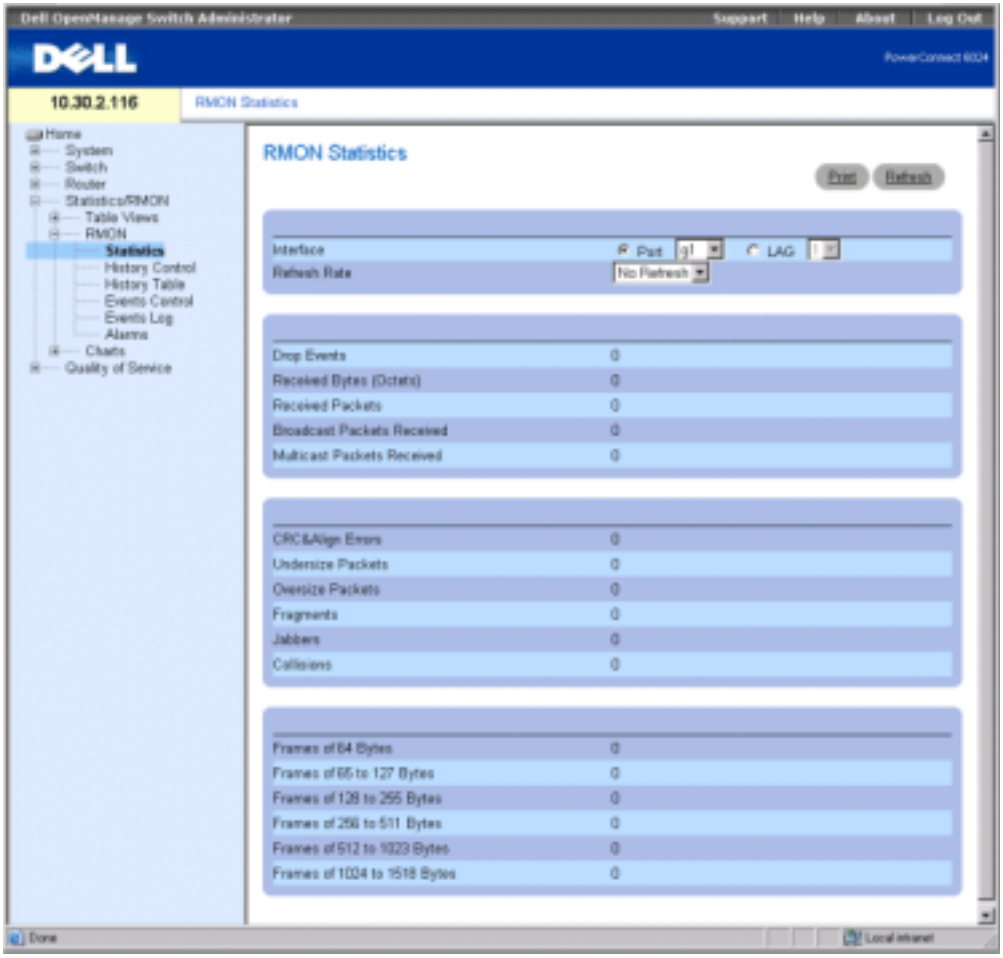
Remote monitoring (RMON) allows network managers to view network information from a remote location. To open the **RMON** page, click **Statistics/RMON→RMON** in the tree view.

Viewing RMON Statistics Group

Use the **RMON Statistics Group** page to display information about device utilization and errors that occurred on the device.

To open the page, click **Statistics/RMON→RMON→Statistics** in the tree view.

Figure 9-7. RMON Statistics Group Page



Interface — Specifies the port or LAG for which statistics are displayed.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Drop Events — Number of dropped events that have occurred on the interface since the device was last refreshed.

Received Bytes (Octets) — Number of octets received on the interface since the device was last refreshed. This number includes bad packets and FCS octets, but excludes framing bits.

Received Packets — Number of packets received on the interface, including bad packets, multicast and broadcast packets, since the device was last refreshed.

Broadcast Packets Received — Number of good broadcast packets received on the interface since the device was last refreshed. This number does not include multicast packets.

Multicast Packets Received — Number of good Multicast packets received on the interface since the device was last refreshed.

CRC & Align Errors — Number of CRC and Align errors that have occurred on the interface since the device was last refreshed.

Undersize Packets — Number of undersized packets (less than 64 octets) received on the interface since the device was last refreshed.

Oversize Packets — Number of oversized packets (over 1518 octets) received on the interface since the device was last refreshed.

Fragments — Number of fragments (packets with less than 64 octets, excluding framing bits, but including FCS octets) received on the interface since the device was last refreshed.

Jabbers — Number of packets received that were more than 1,518 octets long and had a FCS during the sampling session.

Collisions — Number of collisions received on the interface since the device was last refreshed.

Frames of *xx* Bytes — Number of *xx*-byte frames received on the interface since the device was last refreshed.

Viewing Interface Statistics

1. Open the **RMON Statistics Group** page.
2. Select an interface type and number in the **Interface** field.

Viewing RMON Statistics Using the CLI Commands

The following table contains the CLI commands for viewing RMON statistics.

Table 9-4. RMON Statistics CLI Commands

CLI Command	Description
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays RMON Ethernet statistics.

The following is an example of the CLI commands:

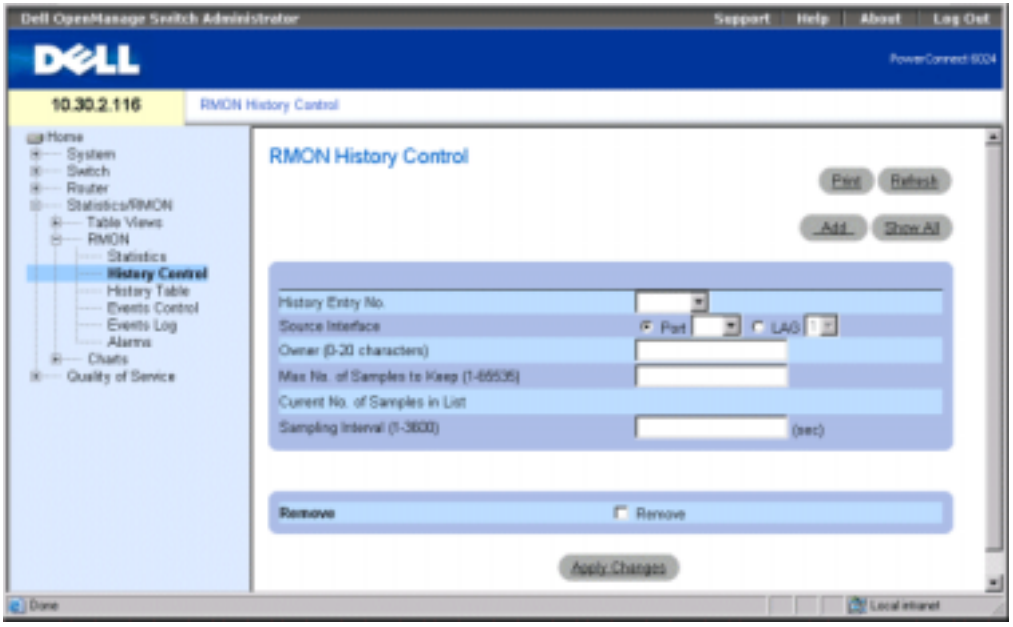
```
Console# show rmon statistics ethernet g1

Port g1

Dropped: 8

Octets: 878128 Packets: 978
```

```
Broadcast: 7 Multicast: 1
CRC Align Errors: 0 Collisions: 0
Undersize Pkts: 0 Oversize Pkts: 0
Fragments: 0 Jabbers: 0
64 Octets: 98 65 to 127 Octets: 0
128 to 255 Octets: 0 256 to 511 Octets: 0
512 to 1023 Octets: 491 1024 to 1518 Octets: 389
```

Viewing RMON History Control Statistics

The **RMON History Control** page contains information about samples of data taken from ports. For example, the samples may include interface definitions or polling periods To open the page, click **Statistics/RMON→RMON→RMON History Control** in the tree view.

Figure 9-8. RMON History Control Page



History Entry No. — Entry number on the **RMON History Control Table**.

Source Interface — Port or LAG from which the history samples were taken.

Owner — RMON station or user that requested the RMON information.

Max No. of Samples to Keep (1-65535) — Number of samples to be saved. The default value is 50.

Current No. of Samples in List — Indicates the current number of samples taken.

Sampling Interval (1-3600) —Indicates in seconds the time that samplings are taken from the ports. The possible values are 1-3600 seconds. The default is 1800 seconds (30 minutes).

Remove — When checked, removes the **RMON History Control Table** entry.

Adding a History Control Entry

1. Open the **RMON History Control** page.
2. Click **Add** to display the **Add History Entry** page.
3. Complete the fields in the dialog and click **Apply Changes**.

   The entry is added to the **RMON History Control Table**.

Modifying a RMON History Control Table Entry

1. Open the **RMON History Control** page.
2. Select an entry in the **History Entry No.** field.
3. Modify the fields as desired and click **Apply Changes**.

   The table entry is modified, and the device is updated.

Deleting a History Control Table Entry

1. Open the **RMON History Control** page.
2. Select an entry in the **History Entry No.** field.
3. Click **Remove** and then click **Apply Changes**.

   The table entry is deleted, and the device is updated.

Viewing RMON History Control Using the CLI Commands

The following table contains the CLI commands for viewing GVRP statistics.

Table 9-5. RMON History CLI Commands

CLI Command	Description
`rmon collection history index [owner ownername | buckets bucket-number] [interval seconds]`	Enables and configures RMON on an interface.
`show rmon collection history [ethernet interface | port-channel port-channel-number]`	Displays RMON collection history statistics.

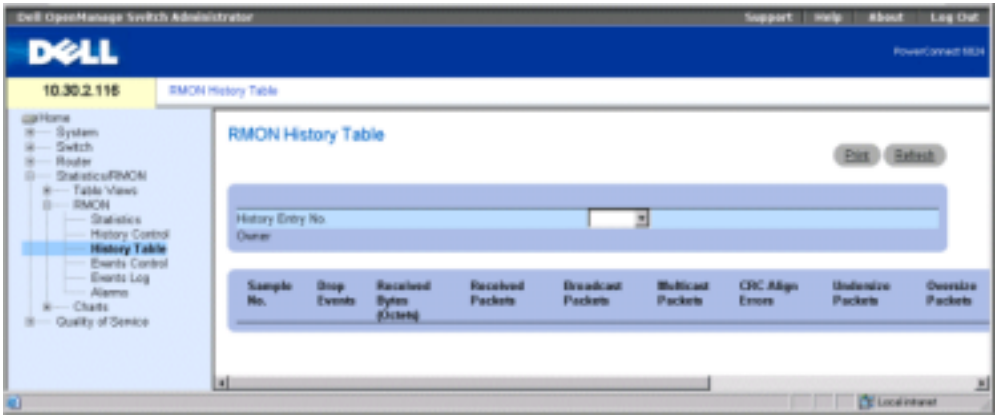
The following is an example of the CLI commands:

```
Console (config)# interface ethernet g8
Console (config-if)# rmon collection history 1 interval 2400
Console (config-if)# exit
Console (config)# exit
Console# disable
Console> show rmon collection history
Index Interface Interval Requested Samples Granted Samples Owner
----- --------- -------- ---------------- -------------- --------
11    10        0        50                50              CLI
```

Viewing the RMON History Table

The RMON History Table page contains interface specific statistical network samplings. Each table entry represents all counter values compiled during a single sample. To open the **RMON History Table** page, click **Statistics/RMON→RMON→History Table** in the tree view.

Figure 9-9. RMON History Table



NOTE: Not all fields are shown in the RMON History Table.

History Entry No. — Contains a list of entry numbers on the **RMON History Control Table**.

Owner — If available, RMON statistics group owner name.

Sample No. — Indicates the specific sample the information in the table reflects.

Drop Events — The number of dropped packets due to lack of network resources during the sampling interval. This may not represent the exact number of dropped packets, but rather the number of times dropped packets were detected.

Received Bytes (Octets)— The number of data octets, including bad packets, received on the network.

Received Packets — The number of packets received during the sampling interval.

Broadcast Packets — The number of good broadcast packets received during the sampling interval.

Multicast Packets — The number of good multicast packets received during the sampling interval.

CRC Align Errors — The number of packets received during the sampling session with a length 64-1,518 octets. However, the packets has a bad packet Check Sequence (FCS) with an integral number of octets or a bad FCS with a non-integral number.

Undersize Packets — The number of packets received less than 64 octets long during the sampling session.

Oversize Packets — The number of packets received more than 1,518 octets long during the sampling session.

Fragments — The number of packets received less than 64 octets long and had a FCS during the sampling session.

Jabbers — The number of packets received more than 1,518 octets long and had a FCS during the sampling session.

Collisions — Estimates the total number of packet collision that occurred during the sampling session. Collision are detected when repeater ports detects two or more stations transmit simultaneously.

Utilization — Estimates the main physical layer network usage on an interface during the session sampling. The value is reflected hundredths of percent.

Viewing Statistics for a Specific History Entry

1. Open the **RMON History Table** page.
2. Select an entry in the **History Entry No.** field.

   The entry's statistics are displayed in the RMON History Table.

Viewing RMON History Control Using the CLI Commands

The following table contains the CLI commands for viewing RMON history.

Table 9-6. RMON History Control CLI Commands

CLI Command	Description
show rmon history *index* {**throughput** | **errors** | **other**} [**period** *seconds*]	Displays RMON Ethernet statistics history.

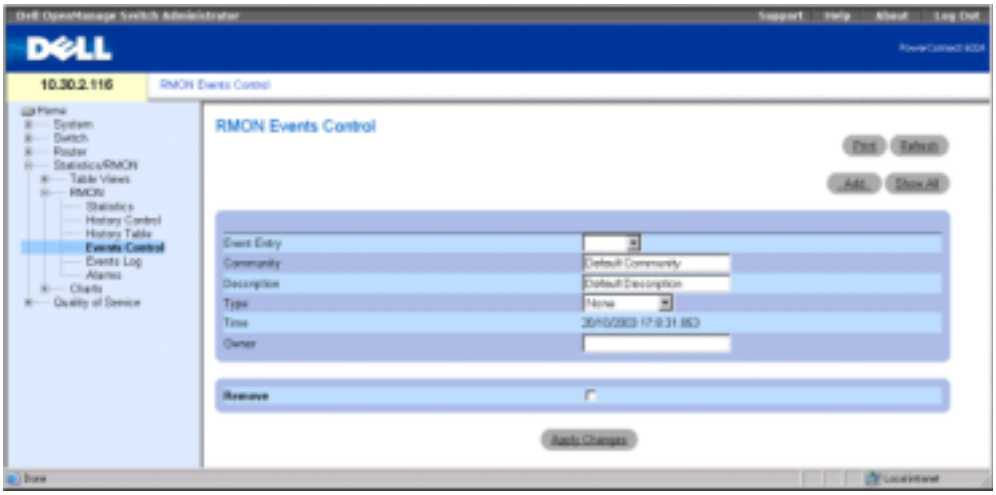
The following is an example of the CLI commands for displaying RMON ethernet statistics for throughput on index 1:

```
Console# show rmon history 1 throughput

Sample Set: 5Owner: cli

Interface:  24interval: 10

Requested samples: 50Granted samples: 50

Maximum table size: 270

Time                 Octets PacketsBroadcast Multicast%

------------------   ------ --------------- --------------

09-Mar-2003 18:29:32 00     00              0

09-Mar-2003 18:29:42 00     00              0

09-Mar-2003 18:29:52 00     00              0

09-Mar-2003 18:30:02 00     00              0

09-Mar-2003 18:30:12 00     00              0

09-Mar-2003 18:30:22 00     00              0
```

Defining Device RMON Events

Use the **RMON Events Control** page to define RMON events. To open the page, click **Statistics/RMON→RMON→Events Control** in the tree view.

Figure 9-10. RMON Events Control Page



Event Entry — Indicates the event.

Community — Community to which the event belongs.

Description — User-defined event description.

Type — Describes the event type. Possible values are:

Log — Event type is a log entry.

Trap — Event type is a trap.

Log and Trap — Event type is both a log entry and a trap.

None — There is no event.

Time — Time when the event occurred.

Owner — The device or user that defined the event.

Remove — When checked, removes the event from the Events Table.

Adding a RMON Event

1. Open the **RMON Events Control** page.
2. Click **Add** to display the **Add an Event Entry** page.
3. Complete the information in the dialog and click **Apply Changes**.
   The event is added to the **RMON Event Table**, and the device is updated.

Modifying a RMON Event

1. Open the **RMON Events Control** page.
2. Select an entry in the **Event Entry** field.
3. Modify the fields in the page and click **Apply Changes**.

   The **RMON Events Table** entry is modified, and the device is updated.

Deleting RMON Event Entries

1. Open the **RMON Events Control** page.
2. Click **Show All** to display the **RMON Events Table**.
3. Click **Remove** for the event(s) you want to delete and then click **Apply Changes**.

   The table entry is deleted, and the device is updated.

NOTE: You can remove a single event entry from the **RMON Events Control** page by clicking the **Remove** check box on that page.

Defining Device Events Using the CLI Commands

The following table contains the CLI commands for defining device events.

Table 9-7. Device Event Definition CLI Commands

CLI Command	Description
`rmon event` *`index type`* `[community` *`text`*`] [description` *`text`*`] [owner` *`name`*`]`	Configures RMON events.
`show rmon events`	Displays RMON event table.

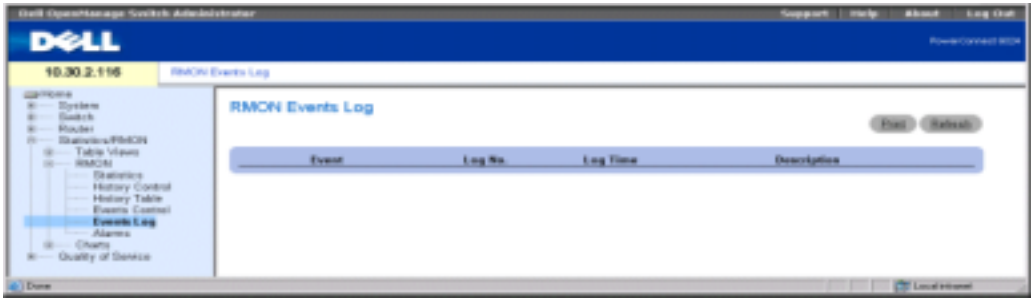
The following is an example of the CLI commands:

```
Console (config)# rmon event 10 log

Console (config)# exit

Console# disable

Console> show rmon events

Index Description Type Community Owner Last time sent

----- --------------- --------- ------ -------------------------

1     Errors            Log         CLI          Jan 18 2002 23:58:17

2    High BroadcastLog-Traprouter    Manager     Jan 18 2002 23:59:48
```

Viewing the RMON Events Log

The **RMON Events Log** page contains a list of RMON events. To open the page, click **Statistics/RMON→RMON→Events Log** in the tree view.

Figure 9-11. RMON Events Log Page



Event — The RMON Events Log entry number.

Log No.— The log number.

Log Time — Time when the log entry was entered.

Description — Describes the log entry.

Defining Device Events Using the CLI Commands

The following table contains the CLI commands for defining device events.

Table 9-8. Device Event Definition CLI Commands

CLI Command	Description
`show rmon log [event]`	Displays the RMON logging table.

The following is an example of the CLI commands:

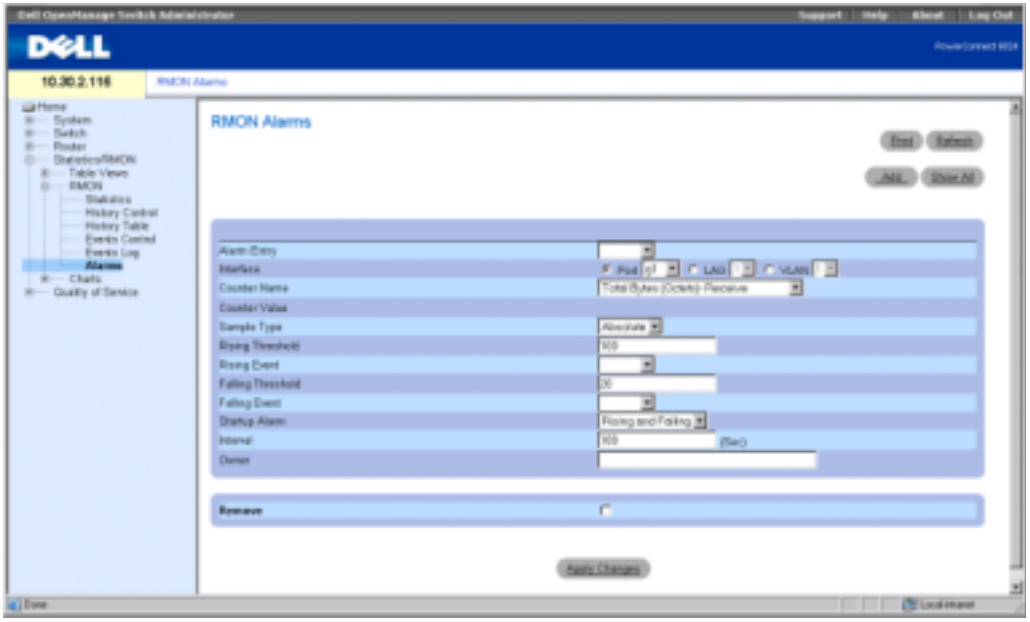
```
Console> show rmon log

Maximum table size: 500

Event Description     Time

----- --------------- -------------

1    Errors           Jan 18 2002 23:48:19

1    Errors           Jan 18 2002 23:58:17

2    High Broadcast   Jan 18 2002 23:59:48
```

Defining RMON Device Alarms

Use the **RMON Alarms** page to set network alarms. Network alarms occur when a network problem, or event, is detected. Rising and falling thresholds generate events. For more information about events, see "Viewing the RMON Events Log."

To open the page, click **Statistics/RMON→RMON→Alarms** in the tree view.

Figure 9-12. RMON Alarms Page



Alarm Entry—Indicates a specific alarm.

Interface—Indicates the interface for which RMON statistics are displayed.

Counter Name—Indicates the selected MIB variable.

Counter Value — The value of the selected MIB variable.

Sample Type—Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible field values are:

Delta — Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold.

Absolute — Compares the values directly with the thresholds at the end of the sampling interval.

Rising Threshold — The rising counter value that triggers the rising threshold alarm. The rising threshold is presented on top of the graph bars. Each monitored variable is designated a color.

Rising /Falling Event — The mechanism in which the alarms are reported, including a log, a trap, or both. When a log is selected, there is no saving mechanism either in the device or in the management system. However, if the device is not being reset, the event remains in the device Log table. If a trap is selected, an SNMP trap is generated and reported via the Trap mechanism. The trap can be saved using the same mechanism.

Falling Threshold — The falling counter value that triggers the falling threshold alarm. The falling threshold is graphically presented on top of the graph bars. Each monitored variable is designated a color.

Startup Alarm — The trigger that activates the alarm generation. Rising is defined by crossing the threshold from a low-value threshold to a higher-value threshold.

Interval (sec)— Alarm interval time.

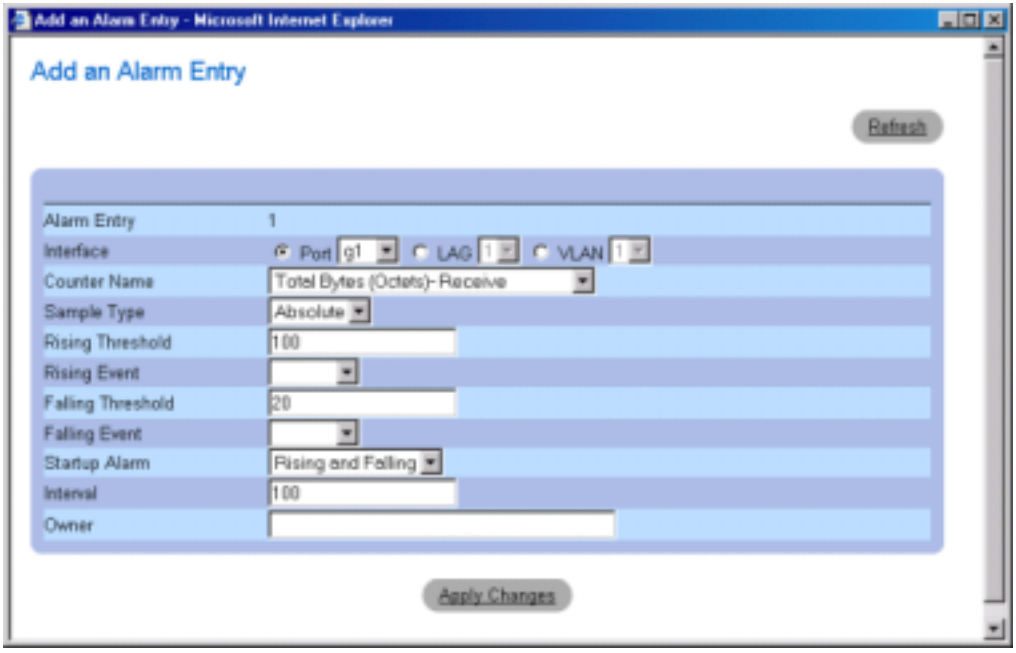
Owner — Device or user that defined the alarm.

Remove — When checked, removes an RMON Alarm.

Adding an Alarm Table Entry

1. Open the **RMON Alarms** page.
2. Click **Add** to display the **Add an Alarm Entry** page.

Figure 9-13. Add an Alarm Entry Page



3 Select an interface.

4 Complete the fields in the dialog and click **Apply Changes**.

The RMON alarm is added, and the device is updated.

Modifying an Alarm Table Entry

1 Open the **RMON Alarms** page.

2 Select an entry in the **Alarm Entry** drop-down menu.

3 Modify the fields in the dialog as desired and click **Apply Changes**.

The entry is modified, and the device is updated.

Displaying the Alarm Table

1 Open the **RMON Alarms** page.

2 Click **Show All** to display the **RMON Alarms Table**.

Deleting an Alarm Table Entry

1 Open the **RMON Alarms** page.

2 Select an entry in the **Alarm Entry** drop-down menu.

3 Check the **Remove** check box and click **Apply Changes**.

The entry is deleted, and the device is updated.

Defining Device Alarms Using the CLI Commands

The following table contains the CLI commands for defining device alarms.

Table 9-9. Device Alarm CLI Commands

CLI Command	Description
`rmon alarm` *`index MIB_Object_ID interval rthreshold fthreshold revent fevent`* `[type` *`type`*`] [startup` *`direction`*`] [owner` *`name`*`]`	Configures RMON alarm conditions.
`show rmon alarm-table`	Displays summary of the alarm table.
`show rmon alarm`	Displays RMON alarm configuration.

The following is an example of the CLI commands:

```
Console (config)# rmon alarm 1000 1.3.6.1.2.1.2.2.1.10.1 360000
1000000 1000000 10 20

Console# show rmon alarm-table

Index                       OID              Owner

----------------------------                 -----

11.3.6.1.2.1.2.2.1.10.1                      CLI

21.3.6.1.2.1.2.2.1.10.1                      Manager

31.3.6.1.2.1.2.2.1.10.9                      CLI
```

Viewing Charts

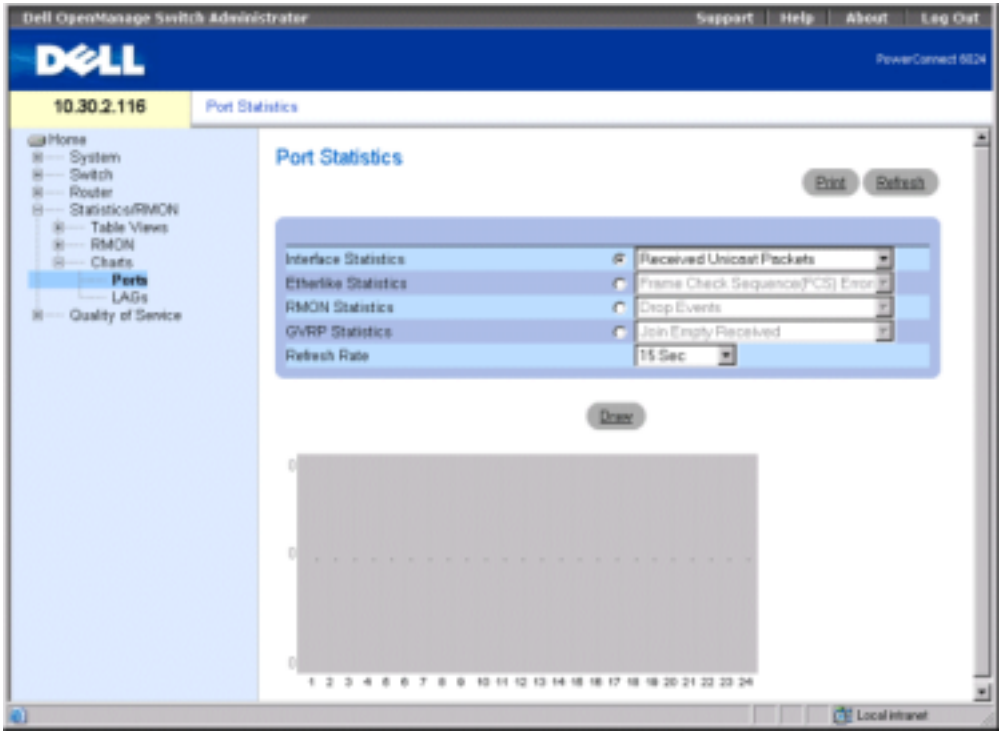
The **Chart** page contains links for displaying statistics in a chart form. To open the page, click **Statistics/RMON→Charts** in the tree view.

Viewing Port Statistics

Use the **Port Statistics** page to display statistics in a chart form for port elements.

To open the page, click **Statistics/RMON→Charts→Ports** in the tree view.

Figure 9-14. Port Statistics Page



Interface Statistics — Selects the type of interface statistics to display.

Etherlike Statistics — Selects the type of Etherlike statistics to display.

RMON Statistics — Selects the type of RMON statistics to display.

GVRP Statistics — Selects the type of GVRP statistics to display.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Displaying Port Statistics

1. Open the **Port Statistics** page.
2. Select the type of statistic to display.
3. Select the desired refresh rate from the **Refresh Rate** drop-down menu.
4. Click **Draw**.

   The graph for the selected statistic is displayed.

Viewing Port Statistics Using the CLI Commands

The following table contains the CLI commands for viewing port statistics.

Table 9-10. Port Statistic CLI Commands

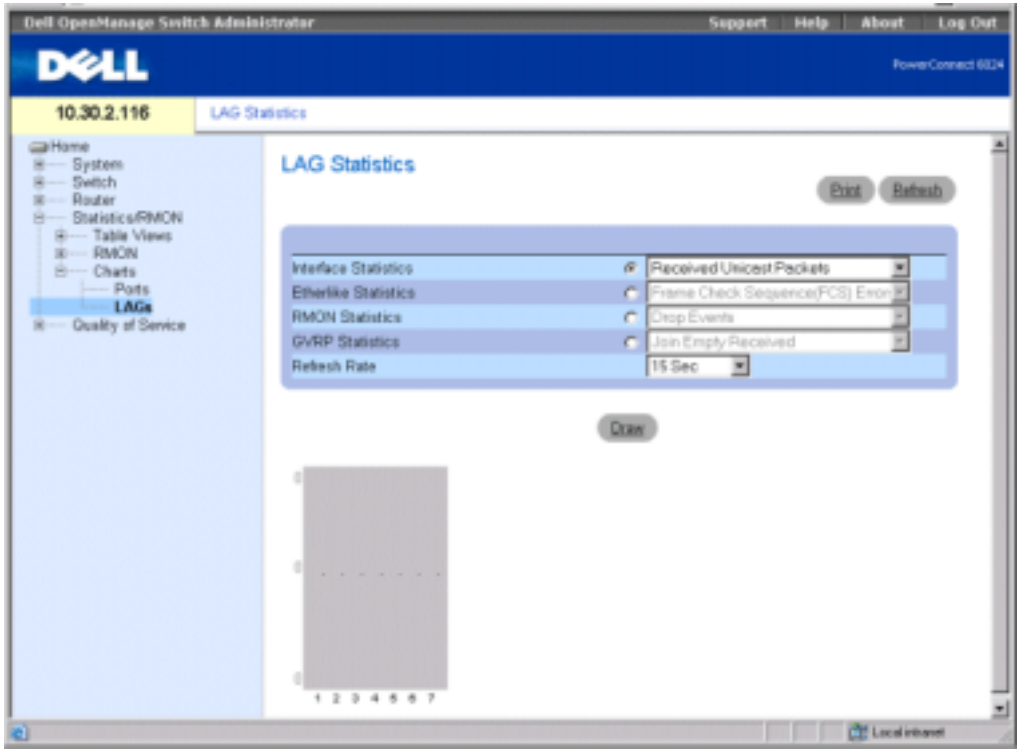
CLI Command	Description
`show interfaces counters [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays traffic seen by the physical interface.
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays RMON Ethernet statistics.
`show gvrp statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays GVRP statistics.
`show gvrp-error statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays GVRP error statistics.

Viewing LAG Statistics

Use the **LAG Statistics** page to display statistics in a chart form for LAGs.

To open the page, click **Statistics/RMON→Charts→LAGs** in the tree view.

Figure 9-15. LAG Statistics Page



Interface Statistics — Selects the type of interface statistics to display.

Etherlike Statistics — Selects the type of Etherlike statistics to display.

RMON Statistics — Selects the type of RMON statistics to display.

GVRP Statistics — Selects the type of GVRP statistics to display.

Refresh Rate — Amount of time that passes before statistics are refreshed. The possible field values are No Refresh, 15, 30 and 60 seconds.

Displaying LAG Statistics

1. Open the **LAG Statistics** page.
2. Select the type of statistic to display.
3. Select the desired refresh rate from the **Refresh Rate** drop-down menu.
4. Click **Draw**.

   The graph for the selected statistic is displayed.

Viewing LAG Statistics Using the CLI Commands

The following table contains the CLI commands for viewing LAG statistics.

Table 9-11. LAG Statistic CLI Commands

CLI Command	Description
`show interfaces counters [ethernet` *`interface`* `| port-channel` *`port-channel-number`*`]`	Displays traffic seen by the physical interface.
`show rmon statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays RMON Ethernet statistics.
`show gvrp statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays GVRP statistics.
`show gvrp-error statistics {ethernet` *`interface`* `| port-channel` *`port-channel-number`*`}`	Displays GVRP error statistics.

10

Configuring Quality of Service

The **Quality of Service** page contains links to the main QoS configuration pages. To open the page, click **Quality of Service** in the tree view.

Quality of Service Overview

Network traffic is usually unpredictable, and the only basic assurance that a network administrator can offer is best effort traffic delivery. To overcome this challenge, network administrators apply Quality of Service (QoS) throughout the network. This ensures that network traffic is prioritized according to specified criteria, and that specific traffic receives preferential treatment. QoS in the network optimizes network performance and entails two basic facilities:

- Classifying incoming traffic into handling classes, based on an attribute, including:
  - The ingress interface
  - Packet content
  - A combination of these attributes
- Providing various mechanisms for determining the allocation of network resources to different handling classes, including:
  - The assignment of network traffic to a particular hardware queue
  - The assignment of internal resources
  - Traffic shaping

In this document, the terms *Class of Service* (CoS) and QoS are used in the following context:

- CoS provides varying Layer 2 traffic services. CoS refers to classification of traffic to traffic-classes, which are handled as an aggregate whole, with no per-flow settings. CoS is usually related to the 802.1p service that classifies flows according to their Layer 2 priority, as set in the VLAN header.
- QoS refers to Layer 2 traffic and above. QoS handles per-flow settings, even within a single traffic class.

The QoS facility involves the following elements:

- **Access Control Lists (ACLs)** — Used to decide which traffic is allowed to enter the system, and which is to be dropped. Only traffic that meets this criteria are subject to CoS or QoS settings. ACLs are used in QoS and network security.
- **Traffic Classification** — Classifies each incoming packet as belonging to a given traffic class, based on the packet contents and/or the context.

- **Assignment to Hardware Queues** — Assigns incoming packets to forwarding queues. Packets are sent to a particular queue for handling as a function of the traffic class to which they belong, as defined by the classification mechanism.
- **Traffic Class-Handling Attributes** — Applies QoS/CoS mechanisms to different classes, including:
  - Bandwidth Management
  - Shaping
  - Policing

Access Control Lists

ACLs inspect incoming packets and classify them into logical groups, based on various criteria. ACL groups have specific actions that are carried out on every packet that is classified to the group. ACLs enable actions which include:

- Forward
- Deny
- Deny and disable port

ACLs are used for the following main purposes:

- As a security mechanism, either permitting or denying entry to packets in a group. This mechanism is described in the section on Network Security.
- As a mechanism to classify packets into traffic classes for which various CoS/QoS handling actions are executed.

ACLs contain multiple classification rules and actions. An Access Control Element (ACE) is composed of a single classification rule and its action. A single ACL may contain one or more ACEs.

The order of the ACEs within an ACL is important, as they are applied in a first-fit manner. The ACEs are processed sequentially, starting with the first ACE. When a packet is matched to an ACE classification, the ACE action is performed and the ACL processing terminates. If more than one ACL is to be processed, the default drop action is applied only after processing all the ACLs. The default drop action requires the user to explicitly allow all the traffic that is permitted, including management traffic, such as telnet, HTTP, or SNMP that is directed to the router itself.

Two types of ACLs are defined:

- **IP ACL** — Applies only to IP packets. All classification fields are related to IP packets.
- **MAC ACL** — Applies to any packet, including non-IP packets. Classification fields are based only on Layer 2.

There are two ways to apply ACLs to an interface:

- **Policy** — In this form, ACLs are grouped together into a more complex structure, called a policy. The policy can contain both ACLs and QoS rules. The user can apply the policy to an interface (see "Advanced QoS Mode").
- **Simple** — In the simple form, a single (MAC or IP) ACL is applied to an interface. Although a policy cannot be applied to an interface, it is possible to apply basic QoS rules that classify packets to output queues (see "Basic QoS Mode").

Mapping to Queues

A Trust Behavior can be selected, or the output service fields can be selected, including:

- **VLAN Priority Tags (VPT)** — VPTs are mapped to an output queues based on the VPT. While queue mapping is user-configurable, the VPT default mapping to the output queue is as follows. In the VPT default mapping, Queue 1 has the lowest priority, as shown in the following table:

Table 10-1. VPT Default Mapping Table

VPT Value	Queue Number
0	3
1	1
2	2
3	4
4	5
5	6
6	7
7	8

NOTE: Mapping of the VPT to the output queue is performed on a system-wide basis, and can be *enabled* or *disabled* per port.

- **802.1p Port-Based** — Packets arriving untagged are assigned to a default VPT, which can be set by the user on a per port basis. Once the VPT is assigned, the packet is treated as if it had arrived with this tag. The VPT mapping to the output queue is based on the same user-defined 802.1p tag-based definitions.
- **Layer 3 Predefined Field** — The user can configure the system to use the IP DSCP of the incoming packet to the output priority queues. The mapping of the IP DSCP to priority queue is set on a per system basis. If this mode is active, a non-IP packet will always be classified to the best effort queue. The default mapping is shown in the following table:

Table 10-2. DSCP Default Mapping Table

DSCP Value	Queue Number
0-7	q1 (Lowest Priority)
8-15	q2
16-23	q3
24-31	q4
32-39	q5
40-47	q6
48-55	q7
55-63	q8 (Highest Priority)

NOTE: The DSCP values 3, 11, 19, 27, 35, 43, 51, and 59 are mapped to q1, q2 ... q8. These settings cannot be changed.

- **Layer 4 Predefined Fields**—Configures the system to use the TCP/UDP destination port of the incoming packet to map the packet to the output priority queues. The mapping of the TCP/UDP destination port to a priority queue is set on a per system basis, in two separate tables. It can be *enabled* or *disabled* per port.
- **None**—All traffic is classified to the best effort service.

After packets are assigned to a specific queue, using the chosen classification method various services can be applied. Scheduling for output queues can be configured, including:

- Strict priority.
- Weighted Round Robin (WRR)
- A combination of these methods.

Scheduling schemes are specified per system. WRR weights to the queues can be assigned in any order. The weight settings are available on a per port basis.

For each interface or queue, the following output shaping can also be configured:

- Burst size.
- Committed Information Rate (CIR).
- Actions for over-the-limit traffic.

QoS Modes

QoS is enabled in the PowerConnect 6024/6024F in either basic or advanced QoS mode.

Basic QoS Mode

In basic QoS mode, it is possible to activate one of the Trust modes, including:

- VPT
- DSCP
- TCP
- UDP
- None

In addition, a single MAC-based or IP-based ACL can be attached directly to the interface (see Configuring Network Security for more information). Only packets that have a **Forward** action are assigned to the output queue, based on the specified classification.

By properly configuring the output queues, you can set the following basic mode services:

- **Minimum Delay** — The queue is assigned to a strict priority policy, and traffic is assigned to the highest priority queue.
- **Best Effort** — Traffic is assigned to the lowest priority queue
- **Bandwidth Assignments** — By configuring the WRR scheduling scheme and choosing the right weights, you can assign bandwidths.

Advanced QoS Mode

Advanced QoS mode provides rules for specifying flow classification and assigning rule actions that relate to bandwidth management. The rules are defined in classification control lists (CCL).

CCLs are set according to the classification defined in the ACL, and they cannot be defined until a valid ACL is defined. When CCLs are defined, you can group ACLs and CCLs together in a more complex structure, called a "policy." Policies can be applied to an interface. Policy ACLs/CCLs are applied in the sequence they appear within the policy. Only a single policy can be attached to a port.

In advanced QoS mode, ACLs can be applied directly to an interface. However, a policy and ACL cannot be simultaneously applied to an interface.

After assigning packets to a specific queue, you can apply services such as configuring output queues for the scheduling scheme, or configuring output shaping for burst size, CIR, or CBS per interface or per queue.

Configuration of Services - Examples

You can use advanced QoS mode settings to apply the following services to network traffic:

- **Best Effort** — Traffic is assigned to the lowest priority queue.
- **802.1p** — The VPT value is set according to the classification.
- **IP DSCP** — The value is set according to the classification.

- **Minimum Delay** — The queue is assigned to a strict priority policy, and traffic is assigned to the highest priority queue.
- **Ingress Metering/Rate Limiting** — A maximum bandwidth value is specified beyond which all traffic is dropped. This is done by setting a meter at the input for the maximum bandwidth, and setting the excess policy to drop. In order to effectively configure this service, the total bandwidth on a specific egress port cannot exceed the port rate.

Configuring QoS Global Parameters

The **QoS Global Parameters** page contains links to QoS pages on which QoS is enabled, DSCP values and settings are remapped, network traffic is queued, and traffic classification is defined. To open the page, click **Quality of Service→QoS Global Parameters** in the tree view.

Defining QoS Settings

Use the **QoS Global Settings** page to select the QoS mode, and to configure the default CoS for incoming traffic on a selected interface. To open the page, click **Quality of Service→QoS Global Parameters→QoS Settings** in the tree view.

Figure 10-1. QoS Global Settings Page

QoS Mode — Disables or enables basic or advanced QoS mode. Basic mode is enabled by default.

NOTE: When moving to and from basic or advanced QoS mode, some settings may be lost.

Interface — The port or LAG for which the default CoS policy is defined.

Set Default CoS for Incoming Traffic To — Determines the default CoS value for incoming packets for which a VLAN tag is not defined. The possible field values are **0-7**. The default CoS is **0**.

Selecting a Service Mode

1. Open the **QoS Settings** page.
2. Select a service mode in the **QoS Mode** field.
3. Click **Apply Changes**.

   The QoS mode is selected, and the device is updated.

Setting the Default CoS Value for Incoming Traffic on an Interface

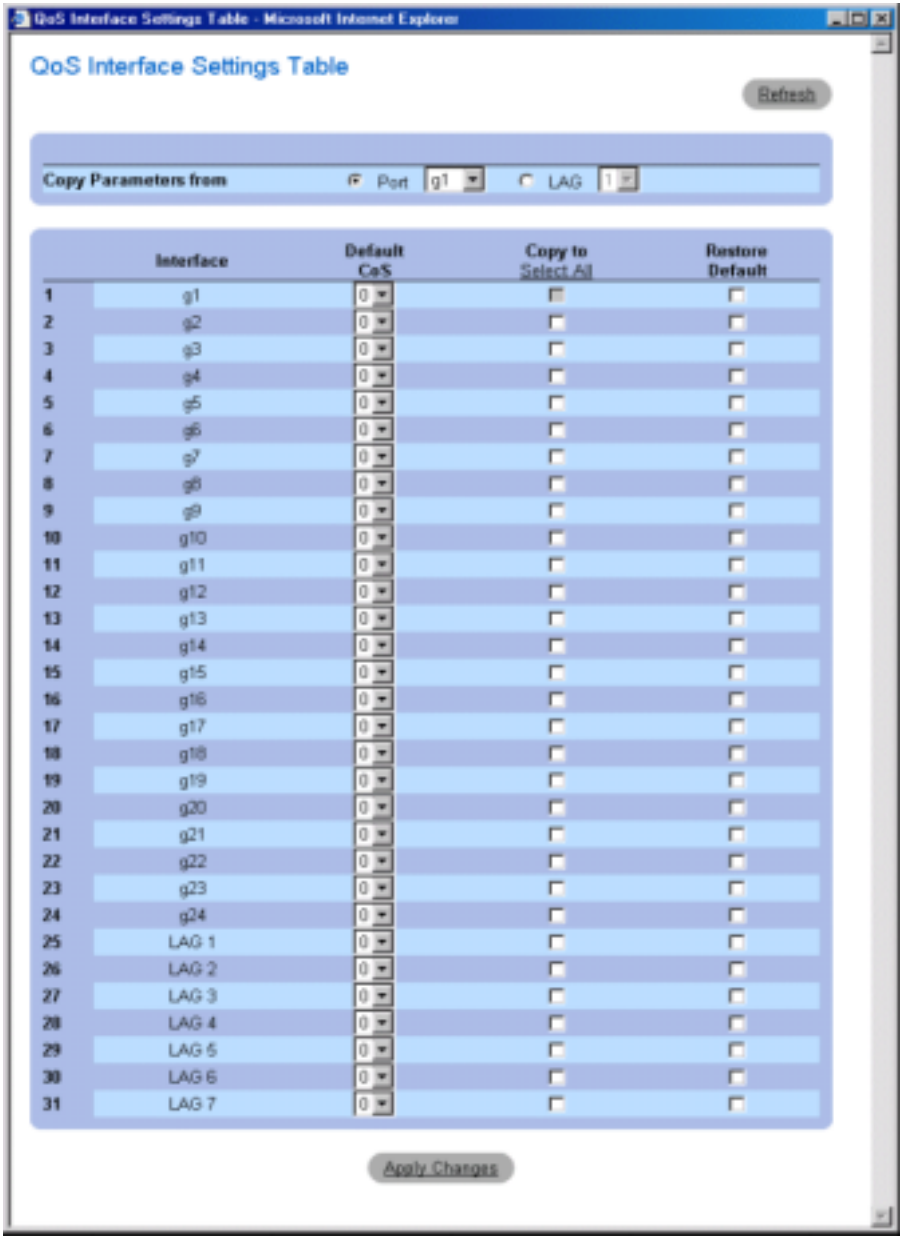
1. Open the **QoS Settings** page.
2. Select an interface, and set the default CoS value for incoming traffic from the drop-down menu.
3. Click **Apply Changes**.

   The default CoS value for incoming traffic on the interface is selected, and the device is updated.

Copying QoS Interface Settings

1. Open the **QoS Settings** page.
2. Click **Show All** to display the **QoS Interface Settings Table** page.
3. Select an interface from which to copy QoS settings to all or any of the interfaces listed in the QoS Interface Settings Table.
4. Check the **Copy to** check box for each interface to which the QoS settings should be copied, or click **Select All** to copy the QoS settings to all listed interfaces.
5. Click **Apply Changes**.

Figure 10-2. QOS Interface Settings Table Page



Defining QoS Settings Using the CLI Commands

Table 10-3. CLI Commands for Defining QoS Settings

CLI Command	Description
`qos [advanced]`	Enables/disables QoS in basic /advanced mode for the entire device.
`show qos`	Displays the QoS mode for the entire device.
`qos cos default-cos`	Configures the default CoS value for the interface.

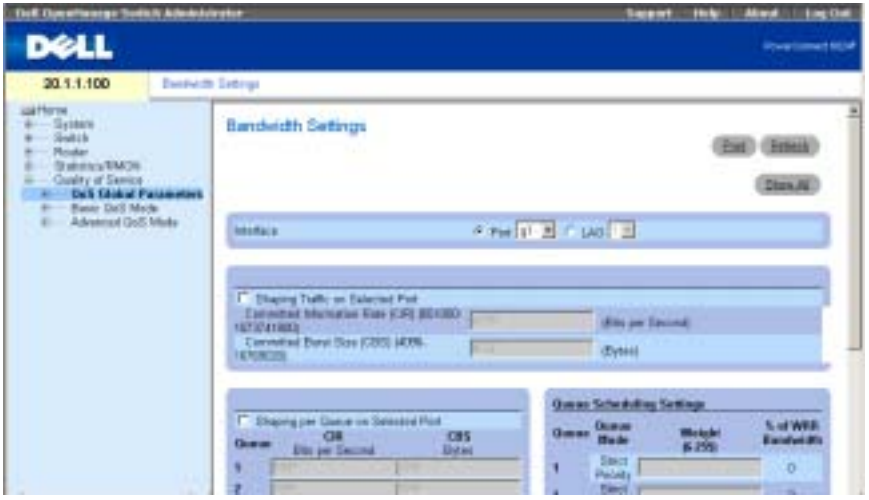
The following is an example of the CLI commands:

```
Console(config)# qos
Console(config)# interface ethernet g5
Console(config-if)# qos cos 3
Console(config-if)# exit
Console(config)# exit
Console# show qos
QoS: basic
Basic trust: vpt
```

Defining Bandwidth Settings

Use the **Bandwidth Settings** page to define the bandwidth settings for a specified ingress interface. Modifying queue scheduling affects the queue settings globally. To open the page, click **Quality of Service→QoS Global Parameters→Bandwidth Settings** in the tree view.

Figure 10-3. Bandwidth Settings



The **Bandwidth Settings** page contains the following fields:

Interface — The port or LAG to which the bandwidth settings apply.

Shaping Traffic on Selected Port — Configures Committed Information Rate (CIR) and Committed Burst Size (CBS) on the interface. It is possible to specify shaping per queue and per interface simultaneously. Shaping is determined by the lower specified value.

Shaping per Queue on Selected Port — Configures CIR and CBS on a per queue basis. It is possible to specify shaping per queue and per interface simultaneously. Shaping is determined by the lower specified value.

Queue Scheduling Settings — Configures weight for each Weighted Round Robin queue.

WRR Weight (0-255) — Assigns weights for each Weighted Round Robin queue. The WRR queues are defined per port and have a range of 6-255. Each queue can be assigned a weight of 0, in which case the queue is not operational and is effectively closed.

Shaping Traffic on a Selected Interface

1. Open the **Bandwidth Settings** page.
2. Select an interface.
3. Check **Shaping Traffic on Selected Port**.

4 Enter values for the interface's CIR and CBS.

5 Click **Apply Changes**.

The CIR and CBS for the selected interface are configured, and the device is updated.

Shaping Traffic on a Per Queue Basis

1 Open the **Bandwidth Settings** page.

2 Select an interface.

3 Check **Shaping per Queue on Selected Port**.

4 Enter CIR and CBS values for each queue.

5 Click **Apply Changes**.

The CIR and CBS for each queue on the selected interface are configured, and the device is updated.

Configuring Queue Scheduling Settings Per Port

1 Open the **Bandwidth Settings** page.

NOTE: Use the **Global Queue Settings** page to modify queue scheduling settings globally.

2 For each of the eight queues, configure the **Strict Priority** setting, or enter a **Weight**.

3 For each queue that has been set system-wide as a WRR queue, enter a weight.

The weight ratio determines the frequency by which the packet scheduler dequeues packets from each queue. The ratio for each queue is defined by the queue weight divided by the sum of all queue weights (normalized weight), thus setting the bandwidth allocation for each queue.

4 Click **Apply Changes**.

The device is updated.

Displaying the Port Bandwidth Settings Table

1 Open the **Bandwidth Settings** page.

2 Click **Show All** to display the **Port Bandwidth Settings Table** page.

Figure 10-4. Port Bandwidth Settings Table

Shaping Type — Can be either per port, per queue, both or none.

Per Port Shaping Rates — CIR and CBS are per port. To view the per queue shaping, use the edit page.

Copying Port Bandwidth Settings

1. Open the **Bandwidth Settings** page.
2. Click **Show All** to display the **Port Bandwidth Settings Table** page.

3 Select an interface from which to copy port bandwidth settings to all or any of the interfaces listed in the Port Bandwidth Settings Table.

4 Check the **Copy to** check box for each interface to which the port bandwidth settings should be copied, or click **Select All** to copy the port bandwidth settings to all listed interfaces.

5 Click **Apply Changes**.

Defining Bandwidth Settings Using the CLI Commands

Table 10-4. Bandwidth Setting CLI Commands

CLI Command	Description
`traffic-shape {committed-rate committed-burst} [queue-id]`	Sets shaper on egress port or queue.
`wrr-queue bandwidth weight1 weight2 ... weight_n`	Assigns Weighted Round Robin (WRR) weights to egress queues.
`priority-queue out num-of-queues number-of-queues`	Configures the number of strict priority queues.
`show qos interface [ethernet interface-number | vlan vlan-id | port-channel number] [buffers | queuing | policers | shapers]`	Displays the QoS interface information.

The following is an example of the CLI commands:

```
Console(config)# interface ethernet g5
Console(config-if)# traffic-shape 124000 96000
Console(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Console(config-if)# exit
Console(config)# priority-queue out num-of-queues 2
Console(config)# exit
Console> show qos interface ethernet g1 buffers
Ethernet g1
Notify Q depth:
qid-size
```

```
1 - 125
2 - 125
3 - 125
4 - 125
5 - 125
6 - 125
7 - 125
8 - 125
qid WRED thresh0 thresh1 thresh2
1   dis  100     100     100
2   dis  100     100     100
3   dis  100     100     100
4   dis  100     100     100
5   Ena  N/A     N/A     N/A
6   Ena  N/A     N/A     N/A
7   Ena  N/A     N/A     N/A
8   Ena  N/A     N/A     N/A
qid MinDP0 MaxDP0 ProbDP0 MinDP1 MaxDP1 ProbDP1 MinDP2 MaxDP2 ProbDP2weight
1   N/A    N/A    N/A     N/A    N/A    N/A     N/A    N/A    N/A    N/A
2   N/A    N/A    N/A     N/A    N/A    N/A     N/A    N/A    N/A    N/A
3   N/A    N/A    N/A     N/A    N/A    N/A     N/A    N/A    N/A    N/A
4   N/A    N/A    N/A     N/A    N/A    N/A     N/A    N/A    N/A    N/A
5    50    60    13   65    80    685    95    4     2
6    50    60    13   65    80    685    95    4     2
7    50    60    13   65    80    685    95    4     2
8    50    60    13   65    80    685    95    4     2
Console> show qos interface ethernet g1 queueing
Ethernet g1
wrr bandwidth weights and EF priority:
```

```
qid-weights Ef - Priority
1 - 125 dis- N/A
2 - 125 dis- N/A
3 - 125 dis- N/A
4 - 125 dis- N/A
5 - N/A ena- 5
6 - 125 dis- N/A
7 - 125 dis- N/A
8 - N/A ena- 8
Cos-queue map:
cos-qid
0 - 3
1 - 1
2 - 2
3 - 4
4 - 5
5 - 6
6 - 7
```

Defining Global Queue Settings

Use the **Global Queue Settings** page to modify queue schedules globally.

To open the page, click **Quality of Service→QoS Global Parameters→Queue Settings** in the tree view.

Figure 10-5. Global Queue Settings

The **Global Queue Settings** page contains the following fields:

Queue — Indicates the queue number.

Strict Priority — Specifies if traffic scheduling is based strictly on the queue priority. This is the default value for queues.

WRR — Specifies if traffic scheduling is based on the Weighted Round Robin (WRR) weights assigned to egress queues. WRR weights are defined in the **Bandwidth Settings** page.

Configuring Queue Scheduling Settings Globally

1. Open the **Global Queue Settings** page.
2. For each of the queues, click **Strict Priority** or **WRR** (weighted round robin).

   The actual WRR settings are set per port on the **Bandwidth Settings** page.

   Checking an option button for any queue automatically selects the scheduling type for the queues after that queue. Every queue before the selected queue uses the opposite type of priority scheduling. For example, if you click **Strict Priority** for queue 6, queues 7 and 8 are also selected as **Strict Priority**; queues 1-5 are selected as **WRR**.

NOTE: A minimum of two queues must be configured as WRR queues.

3. Click **Apply Changes** to update the device.

Defining CoS to Queue Mapping

The **CoS to Queue Mapping Table** page enables mapping CoS values to specific queues. To open the page, click **Quality of Service→QoS Global Parameters→CoS to Queue** in the tree view.

Figure 10-6. CoS to Queue Mapping Table Page

Class of Service — The 802.1Q VLAN priority tag in the incoming packet.

Queue — Maps the CoS to the selected queue. The possible values for the queue are **1**-8.

Incoming packets with the specified CoS value are mapped to the defined queue, if **Trust** was enabled for CoS.

Restore Defaults — Restores all queues to the default class of service settings.

Mapping CoS to Queues

1. Open the **CoS to Queue Mapping Table** page.
2. Select a queue for each **Class of Service** entry.
3. Click **Apply Changes**.

   CoS is mapped to queues, and the device is updated.

Resetting CoS Mapping to the Default Queues:

1. Open the **CoS to Queue Mapping Table** page.
2. Check **Restore Defaults**.
3. Click **Apply Changes**.

The CoS to queues mapping is reset to the default, and the device is updated.

Mapping CoS to Queues Using the CLI Commands

The following table contains the CLI commands for mapping CoS to queues.

Table 10-5. Mapping CoS Queues CLI Commands

CLI Command	Description
`wrr-queue cos-map` *`queue-id cos1 ... cos8`*	Maps assigned CoS values to select one of the egress queues.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Displays all the maps for QoS

The following is an example of the CLI commands:

```
console(config)# wrr-queue cos-map 7 246
console(config)# show qos map dscp-queue
Dscp-queue map:
d1 : d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------------
0  : 01 01 01 01 01 01 01 01 02 02
1  : 02 02 02 02 02 02 03 03 03 03
2  : 03 03 03 03 04 04 04 04 04 04
3  : 04 04 05 05 05 05 05 05 05 05
4  : 06 06 06 06 06 06 06 06 07 07
5  : 07 07 07 07 07 07 08 08 08 08
6  : 08 08 08 08
console(config)# show qos map tcp-port-queue
Tcp port-queue map:
Port queue
----- ------
6000  1
```

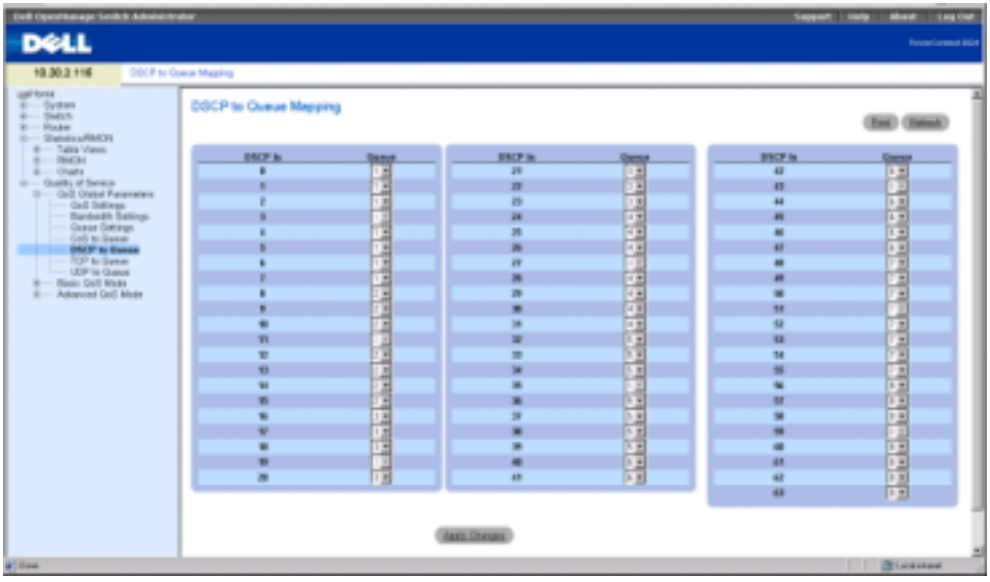
```
6001  2
6002  3
console(config)# show qos map udp-port-queue
Udp port-queue map:
Port queue
----- -----
8000  1
8001  2
console(config)# show qos map dscp-policed
Policed-dscp map:
d1 :d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------------
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
6 : 60 61 62 63
console(config)# show qos map dscp-mutation
Dscp-dscp mutation map:
d1 :d2 0  1  2  3  4  5  6  7  8  9
-----------------------------------------
0 : 00 01 02 03 04 05 06 07 08 09
1 : 10 11 12 13 14 15 16 17 18 19
2 : 20 21 22 23 24 25 26 27 28 29
3 : 30 31 32 33 34 35 36 37 38 39
4 : 40 41 42 43 44 45 46 47 48 49
5 : 50 51 52 53 54 55 56 57 58 59
```

```
6 : 60 61 62 63
```

Defining DSCP to Queue Mapping

The **DSCP to Queue Mapping** page enables mapping DSCP values to specific queues. To open the page, click **Quality of Service→QoS Global Parameters→DSCP to Queue** in the tree view.

Figure 10-7. DSCP to Queue Mapping Page



DSCP In — Indicates the Differentiated Services Code Point value in the incoming packet

Queue — Maps the DSCP value to the selected queue.

Incoming packets with the specified DSCP value are mapped to the designated queue, if **Trust** mode is enabled for DSCP. The DSCP values 3, 11, 19, 27, 35, 43, 51, and 59 are mapped to q1, q2 ... q8. These settings cannot be changed.

Mapping DSCP to Queues

1. Open the **DSCP to Queue Mapping** page.
2. Select a queue for each DSCP level.
3. Click **Apply Changes**.

   DSCP is mapped to queues, and the device is updated.

Mapping DSCP to Queues Using the CLI Commands

Table 10-6. DSCP to Queue CLI Commands

CLI Command	Description
`qos map dscp-queue dscp-list to queue-id`	Modifies the DSCP to CoS map.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Displays all the QoS maps.

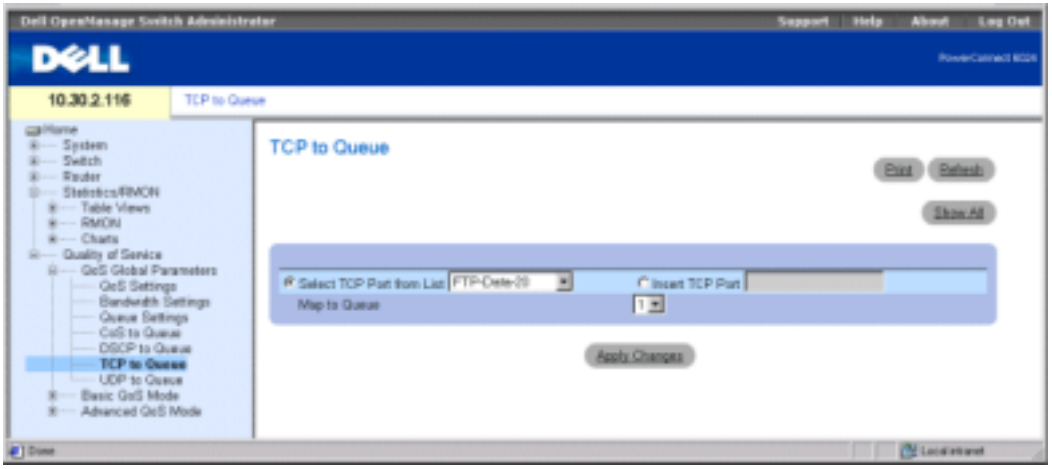
The following is an example of the CLI commands:

```
console(config)# qos map dscp-queue 33 40 41 to 1
console (config) # exit
console # show qos map dscp-queue
Dscp-queue Map
d1:  d2 0 1 2 3 4 5 6 7 8 9
---------------------------
0:   01 01 01 01 01 01 02 02
1:   02 02 02 02 02 03 03 03
2:   03 03 03 04 04 04 04 04
3:   04 04 05 05 05 05 05 05
4:   06 06 06 06 06 06 07 07
5:   07 07 07 07 08 08 08 08
6:   08 08 08 08
```

Defining QoS TCP to Queue Mapping

The **QoS TCP to Queue** page enables mapping a TCP port to a queue. To open the page, click **Quality of Service→QoS Global Parameters→TCP to Queue** in the tree view.

Figure 10-8. QoS TCP to Queue Page



Select TCP Port from List — Selects a known TCP port for mapping to a queue.

Insert TCP Port — Enables manually entering a TCP port for mapping to a queue.

Map to Queue — Indicates the queue to which the specified TCP port is mapped.

Mapping a Known TCP Port to a Queue

1. Open the **TCP to Queue** page.
2. Select the **Select TCP Port from List** option.
3. Select a TCP port.
4. Select a queue from the **Map to Queue** list.
5. Click **Apply Changes**.

   The TCP port is mapped to the specified queue, and the device is updated.

Mapping an Unlisted TCP Port to a Queue

1. Open the **QoS TCP to Queue** page.
2. Select the **Insert TCP Port** option.
3. Enter the TCP port number and description in the **Insert TCP Port** field.
4. Select a queue from the **Map to Queue** list.
5. Click **Apply Changes**.

   The TCP port is mapped to the specified queue, and the device is updated.

Removing TCP to Queue Mapping

1. Open the **QoS TCP to Queue** page.
2. Click **Show All** to display the **TCP to Queue Mapping Table** page.
3. Check the **Remove** check box for each of the TCP ports for which queue mapping is removed.
4. Click **Apply Changes**.

Defining TCP to Queue Mapping Using the CLI Commands

Table 10-7. TCP to Queue Mapping CLI Commands

CLI Command	Description
`qos map tcp-port-queue` *`port1 ... port 8 to queue-id`*	Modifies the TCP-Port to queue.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Displays all the QoS maps.

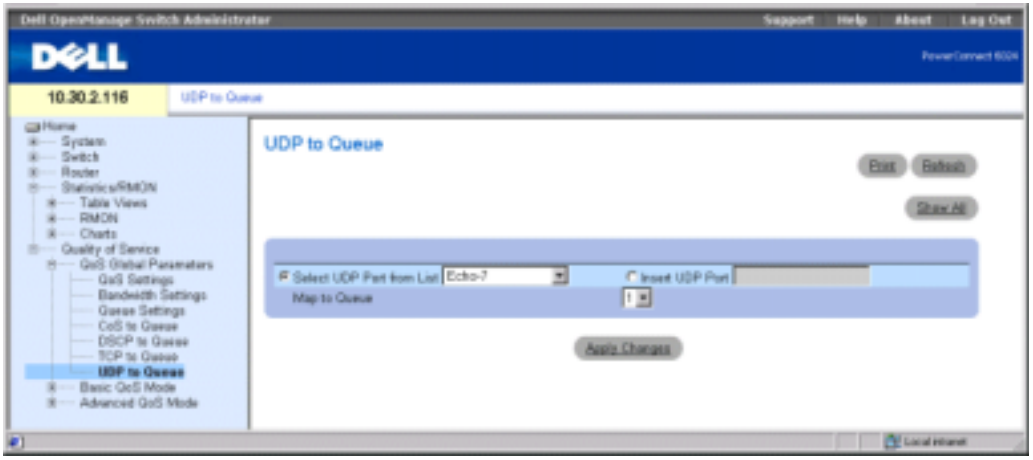
The following is an example of the CLI commands:

```
console(config)# qos map tcp-port-queue 2000 80 to 2
console(config)# exit
console# show qos map tcp-port-queue
Tcp port - queue map
Port         queue
--------------------
6000       1
6001       2
6002       3
```

Defining QoS UDP to Queue Mapping

The **QoS UDP to Queue** page enables mapping of a UDP port to a queue. To open the page, click **Quality of Service→QoS Global Parameters→UDP to Queue** in the tree view.

Figure 10-9. UDP to Queue Page



Select UDP Port from List — Selects a known UDP port for mapping to a queue.

Insert UDP Port — Enables manually entering a UDP port for mapping to a queue.

Map to Queue — The queue to which the specified UDP port is mapped.

Mapping a Known UDP Port to a Queue

1. Open the **UDP to Queue** page.
2. Select the **Select UDP Port from List** option.
3. Select a UDP port.
4. Select a queue from the **Map to Queue** list.
5. Click **Apply Changes**.

   The UDP port is mapped to the specified queue, and the device is updated.

Mapping an Unlisted UDP Port to a Queue

1. Open the **UDP to Queue** page.
2. Select the **Insert UDP Port** option.
3. Enter the UDP port number in the **Insert UDP Port** field.
4. Select a queue from the **Map to Queue** list.
5. Click **Apply Changes**.

   The UDP port is mapped to the specified queue, and the device is updated.

Removing UDP to Queue Mapping

1. Open the **UDP to Queue** page.
2. Click **Show All** to display the **UDP to Queue Mapping Table** page.
3. Click **Remove** for each of the UDP ports for which queue mapping should be removed.
4. Click **Apply Changes**.

Defining UDP to Queue Mapping Using the CLI Commands

Table 10-8. UDP to Queue Mapping CLI Commands

CLI Command	Description
`qos map udp-port-queue` *`port1 ... port 8 to queue-id`*	Modifies the UDP-Port to queue.
`show qos map [dscp-queue | tcp-port-queue | udp-port-queue | dscp-policed | dscp-mutation]`	Displays all the QoS maps.

The following is an example of the CLI commands:

```
console(config)# qos map udp-port-queue 68 to 1
console(config)# exit
console# show qos map udp-port-queue
Udp port-queue map:
Port queue
----- -----
8000  1
8001  2
```

Configuring Basic QoS Mode

The **Basic QoS Mode** page contains links to QoS pages on which Trust Mode and DSCP Rewriting are configured. To open the **Basic QoS Mode** page, click **Quality of Service→Basic QoS Mode** in the tree view.

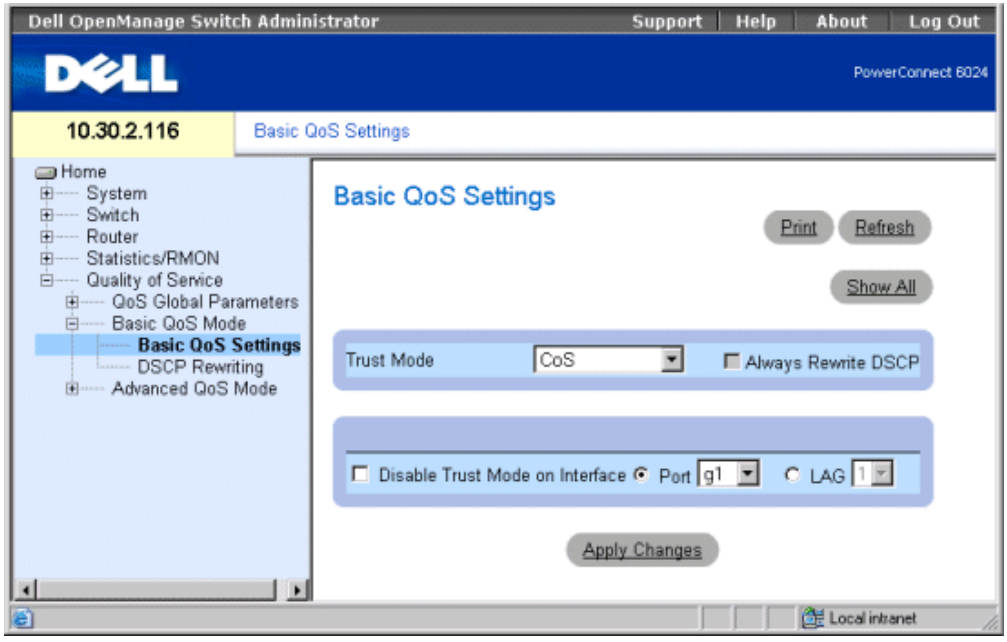
Defining Basic QoS Settings

Use the **Basic QoS Settings** page to configure the Global Trust Mode, which is set on specified interfaces. Packets entering a QoS domain are classified at the edge of the QoS domain. When the packets are classified at the edge, Trust Mode can be configured on ports.

DSCP values can be rewritten at the QoS administrative domain boundary. If two QoS domains have different DSCP definitions, the DSCP values can be rewritten. The DSCP map is applied only to ingress, DSCP-trusted ports.

To open **Basic QoS Settings** page, click **Quality of Service→Basic QoS Mode→Basic QoS Settings** in the tree view.

Figure 10-10. Basic QoS Settings Page



Trust Mode — Selects the trust mode. If a packet's CoS tag, DSCP tag, and TCP/UDP mapping are mapped to different queues, the **Trust Mode** determines the queue to which the packet is assigned. Possible values are:

CoS — Sets trust mode to CoS on the device. The CoS mapping determines the packet queue.

DSCP — Sets trust mode to DSCP on the device. The DSCP mapping determines the packet queue.

TCP/UDP Port — Sets trust mode to TCP/UDP Port on the device. The TCP/UDP Port mapping determines the packet queue.

Always Rewrite DSCP — Rewrites the packet DSCP tag according to the QoS DSCP Rewriting configuration. **Always Rewrite DSCP** can only be checked if the **Trust Mode** is **DSCP**.

Disable Trust Mode on Interface — Disables the trust mode for the select port or LAG.

Interface — Port or LAG on which trust mode is disabled.

Setting the Trust Mode

1. Open the **Basic QoS Settings** page.
2. Select a **Trust Mode**.
3. If the **Trust Mode** is **DSCP**, check **Always Rewrite DSCP** so that the DSCP tags are rewritten as mapped.
4. Click **Apply Changes**.

   The Trust Mode is selected, and the device is updated.

Disabling Trust Mode for Interfaces:

1. Open the **Basic QoS Settings** page.
2. Click **Show All** to display the **Basic QoS Settings Table** page.
3. Check **Disable Trust Mode** for all interfaces on which Trust Mode should be disabled.
4. Click **Apply Changes**.

Defining Basic QoS Settings Using the CLI Commands

Table 10-9. Basic QoS Settings CLI Commands

CLI Command	Description
`qos trust cos | dscp | tcp-udp-port`	In the global context, this command is used to configure the system to basic mode and the trust state.
`qos trust`	In the interface configuration context, this command is used to enable each port trust state.
`qos dscp-mutation`	Applies the DSCP mutation map to a system DSCP trusted port (always rewrites DSCP on this port).

The following is an example of the CLI commands:

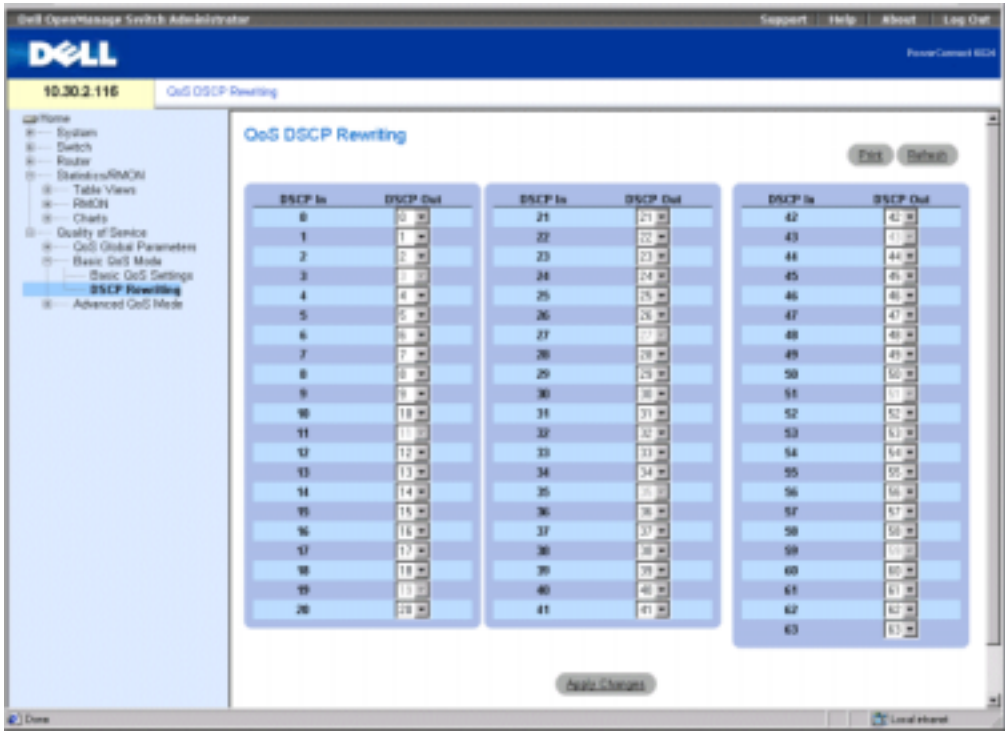
```
console(config)# qos trust dscp
console(config)# qos dscp-mutation
```

```
Console (config)# interface ethernet g5
Console (config-if) qos trust
```

Defining QoS DSCP Rewriting Settings

Use the **QoS DSCP Rewriting** page to configure the method for rewriting DSCP tags. To open the page, click **Quality of Service→Basic QoS Settings→DSCP Rewriting** in the tree view.

Figure 10-11. QoS DSCP Rewriting Page



DSCP In — DSCP tag on an incoming packet.

DSCP Out — DSCP tag on outgoing packets.

Configuring DSCP Rewriting

1. Open the **QoS DSCP Rewriting** page.
2. For each of the **DSCP In** tags, select a **DSCP Out** value from the drop-down list.
3. Click **Apply Changes**.

   DSCP rewriting is configured, and the device is updated.

Configuring DSCP Rewriting Using the CLI Commands

Table 10-10. DSCP Rewriting CLI Commands

CLI Command	Description
`qos map dscp-mutation` *in-dscp* `to` *out-dscp*	Modifies the DSCP to DSCP mutation map.

The following is an example of the CLI commands to define DSCP mutation map:

```
console(config)# qos map dscp-mutation 1 2 4 5 6 to 63
```

Configuring Advanced QoS Mode

The **Advanced QoS Mode** page contains links to QoS pages for configuring advanced settings. To open the page, click **Quality of Service→Advanced QoS Mode** in the tree view.

Defining QoS DSCP Mapping Settings

When traffic exceeds user-defined limits, use the **QoS DSCP Mapping** page to configure the DSCP tag to use in place of the incoming DSCP tags. To open the page, click **Quality of Service→ Advanced QoS Mode→DSCP Mapping** in the tree view.

Figure 10-12. QoS DSCP Mapping Page

DSCP In — DSCP tag on an incoming packet.

Out of Profile DSCP — Sets a new DSCP tag to incoming tag.

Configuring DSCP Mapping

1. Open the **QoS DSCP Mapping** page.
2. Select a value from the **Out of Profile DSCP** drop-down menu.
   This value replaces the **DSCP In** tag value.
3. Click **Apply Changes**.
   DSCP mapping is configured, and the device is updated.

Configuring DSCP Mapping Using the CLI Commands

Table 10-11. DSCP Mapping CLI Commands

CLI Command	Description
`qos map policed-dscp dscp-list to dscp-mark-down`	Modifies the policed DSCP map for remarking.

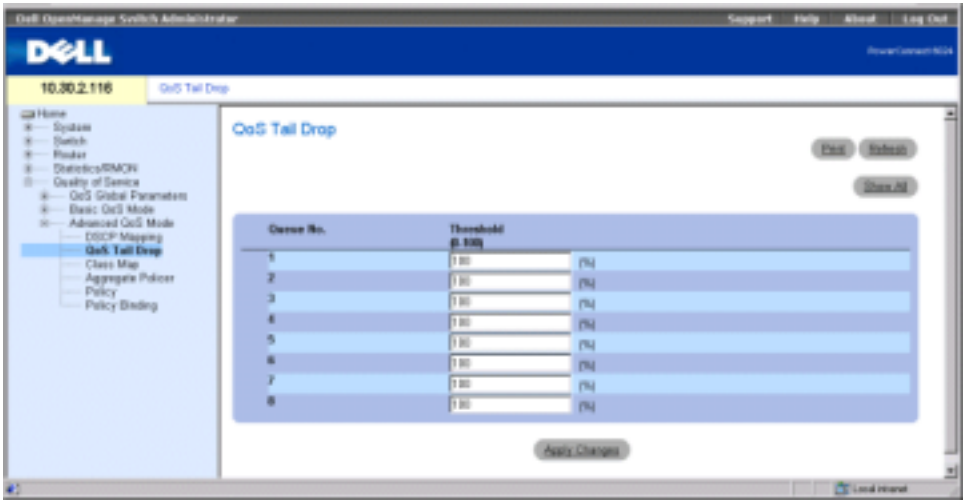
The following is an example of the CLI commands to map DSCP values 12 and 18 to value 56, when out of profile:

```
console(config)# qos map policed-dscp 12 18 to 56
```

Defining QoS Tail Drop Settings

Tail drop occurs when a packet burst saturates a buffer. The last few packets in the burst are dropped, due to lack of space in the buffer. Use the **QoS Tail Drop** page to define tail drop settings for each queue. To open the **QoS Tail Drop** page, click **Quality of Service→Advanced QoS Mode→ QoS Tail Drop** in the tree view.

Figure 10-13. QoS Tail Drop Page



Queue No.—Specifies the queue for which the tail drop settings apply.

Threshold (1-100) — The tail drop threshold percentage for the queue. The packet refers to this threshold, and if it is exceeded, packets are dropped until the threshold is no longer exceeded.

Setting a Tail Drop Threshold

1. Open the **QoS Tail Drop** page.
2. Select a threshold for each queue.
3. Click **Apply Changes**.

   The tail drop threshold is configured, and the device is updated.

Setting Tail Drop Parameters for an Interface:

1. Open the **QoS Tail Drop** page.
2. Click **Show All** to display the **Tail Drop Table** page.
3. Select a status for each interface.
4. Click **Apply Changes**.
5. The tail drop status is defined for the interfaces.

Defining QoS Tail Drop Settings Using the CLI Commands

Table 10-12. Tail Drop Settings CLI Commands

CLI Command	Description
`qos wrr-queue threshold` *`queue-id threshold-percentage`*	Assigns tail-drop thresholds.

The following is an example of the CLI commands to define tail drop settings:

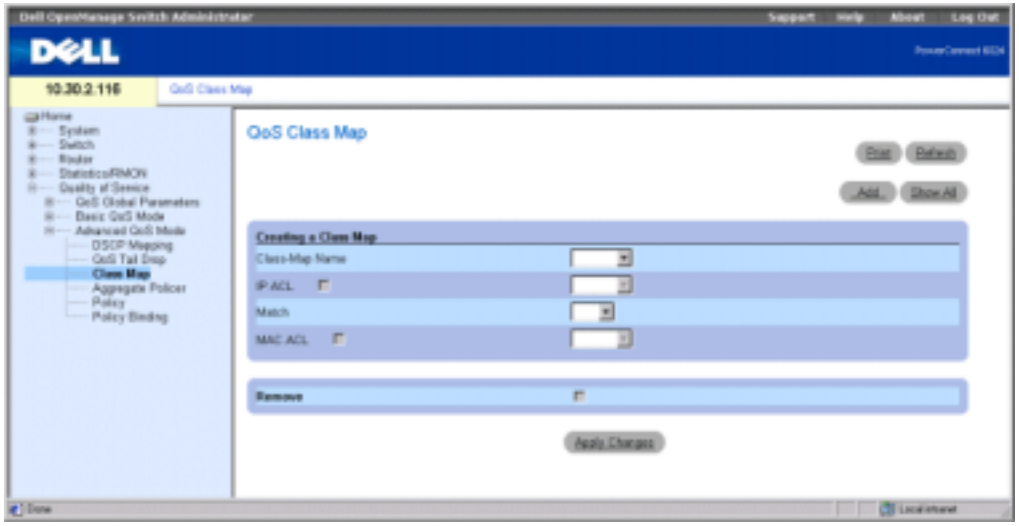
```
console(config)#qos wrr-queue threshold 8 80
```

Defining QoS Class Maps

One IP ACL and/or one MAC ACL comprise a class map. Class maps are configured to match packet criteria, and are matched to packets on a first-fit basis. For example, Class Map A is assigned packets based only on an IP-based ACL or a MAC-based ACL. Class Map B is assigned to packets based on both an IP-based and a MAC-based ACL.

Use the **QoS Class Map** page to enable assigning and editing class maps. To open the page, click **Quality of Service→Advanced QoS Mode→Class Map** in the tree view.

Figure 10-14. QoS Class Map Page



Class-Map Name — The user-defined name of the class map.

IP ACL — The IP ACL from the IP Access Control List (ACL). For more information about defining IP-based ACLs, see "Defining IP based ACLs."

Match — Criteria used to match IP addresses and /or MAC addresses with an ACL's address. Possible values are:

And — Both the MAC-based and the IP-based ACL must match a packet.

Or — Either the MAC-based or the IP-based ACL must match a packet.

MAC ACL — The MAC ACL from the MAC Access Control List. For information about defining MAC-based ACLs, see "Defining MAC based ACLs."

Remove — When checked, removes the class map from the Class Map Table.

Adding a Class Map

1. Open the **QoS Class Map** page.
2. Click **Add** to display the **Add a Class-Map** page.
3. Enter a name (16 characters maximum) for the class map in the **Class-Map Name** field.
4. Do one of the following.
   - To attach an IP ACL to the class map, check **IP ACL** and select an IP ACL from the drop-down menu.
   - To attach a MAC ACL to the class map, check **MAC ACL** and select a MAC ACL from the drop-down menu.

5 Select either **And** or **Or** from the **Match** drop-down menu if both the **IP ACL** and **MAC ACL** check boxes are selected.

6 Click **Apply Changes**.

The class map is created, and the device is updated.

Editing a Class Map

1 Open the **QoS Class Map** page.

2 Select a class map from the **Class-Map Name** drop-down menu.

3 Edit the remaining fields on the page as desired.

4 Click **Apply Changes**.

5 The class map is edited, and the device is updated.

Deleting a Class Map

1 Open the **QoS Class Map** page.

2 Select a class map from the **Class-Map Name** drop-down menu.

3 Check the **Remove** check box.

4 Click **Apply Changes**.

The class map is deleted, and the device is updated.

Displaying the Class Map Table

1 Open the **QoS Class Map** page.

2 Click **Show All** to display the **Class Map Table** page.

Defining QoS Class Maps Using the CLI Commands

Table 10-13. QoS Class Maps CLI Commands

CLI Command	Description
`class-map` *`class-map-name`* `[match-all | match-any]`	Creates a class map and enters class map configuration mode.
`match access-group` *`acl-name`*	Defines the match criterion to classify traffic; active only under class map configuration mode.
`show class-map [`*`class-map-name`*`]`	Displays all the class maps.

The following is an example of the CLI commands:

```
console(config)# class-map class1 match-all
```

```
console(config-cmap)# match access-group dell
console(config-cmap)# exit
console(config)# exit
console> show class-map class1
Class Map match-all class1 (id4)
```

Defining QoS Aggregate Policers

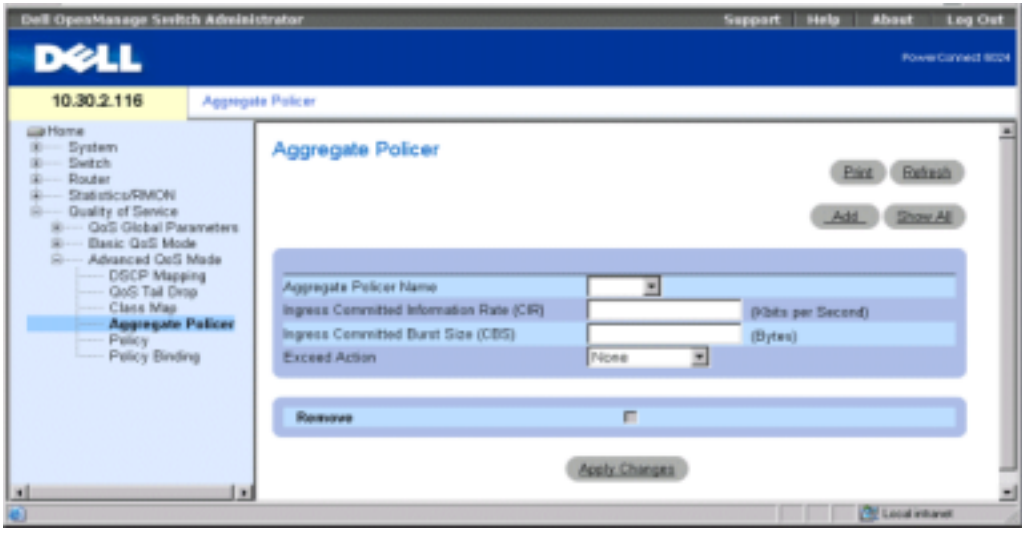
After a packet is classified, the policing process begins. A policer specifies the bandwidth limit for incoming traffic on the classified flow and actions are defined for packets that exceed the limits. These actions include forwarding packets, dropping packets, or remarking packets with a new DSCP value.

Your switch supports per flow and aggregate policers.

Aggregate policers enforce limits on a group of flows. An aggregate policer cannot be deleted if it is being used in a policy map. First delete the aggregate policer from all policy maps by using the **no police aggregate command** before using the **no qos aggregate-policer** command.

Use the **QoS Aggregate Policer** page to specify the bandwidth limits and define actions to take on packets that do not meet the requirements. To open the page, click **Quality of Service→Advanced QoS Mode→Aggregate Policer** in the tree view.

Figure 10-15. QoS Aggregate Policer Page



Aggregate Policer Name—Specifies the aggregate policer name.

Ingress Committed Information Rate (CIR) — CIR in bits per second.

Ingress Committed Burst Size (CBS) — CBS in bytes per second.

Exceed Action — Action assigned to incoming information exceeds the traffic limits. Possible values are:

Drop — Packets exceeding the limits are dropped.

Remark DSCP — Packets exceeding the limits are forwarded with a flagged/remarked DSCP value.

None — Packets exceeding the limits are forwarded.

Remove — When checked, removes the aggregate policer from the Aggregate Policer Table.

Adding an Aggregate Policer

1. Open the **QoS Aggregate Policer** page.
2. Click **Add** to display the **Add Aggregate Policer** page.
3. Complete the fields in the dialog, and click **Apply Changes**.

   The aggregate policer is created, and the device is updated.

Deleting an Aggregate Policer

1. Open the **QoS Aggregate Policer** page.
2. Select an aggregate policer from the drop-down menu.
3. Check **Remove** and then click **Apply Changes**.

   The aggregate policer is deleted, and the device is updated.

Editing an Aggregate Policer:

1. Open the **QoS Aggregate Policer** page.
2. Click **Show All** to display the **Aggregate Policer Table** page.
3. Edit the information in the table for the policers you want to edit.
4. Click **Apply Changes**.

Defining Aggregate Policers Using the CLI Commands

Table 10-14. Aggregate Policer CLI Commands

CLI Command	Description
`qos aggregate-policer` *aggregate-policer-name committed-rate-bps excess-burst-byte exceed-action* {drop | policed-dscp-transmit}	Defines the police parameters that can be applied to multiple traffic classes within the same policy map.
`show qos aggregate police` [*aggregate-policer-name*]	Displays the aggregate policer parameter.

The following is an example of the CLI commands:

```
console# qos aggregate policer policer1 124000 96000 exceed-action
drop

console> show qos aggregate police policer1

aggregate-policer policer1 96000 4800 exceed-action drop

not used by any policy map
```

Defining Policies

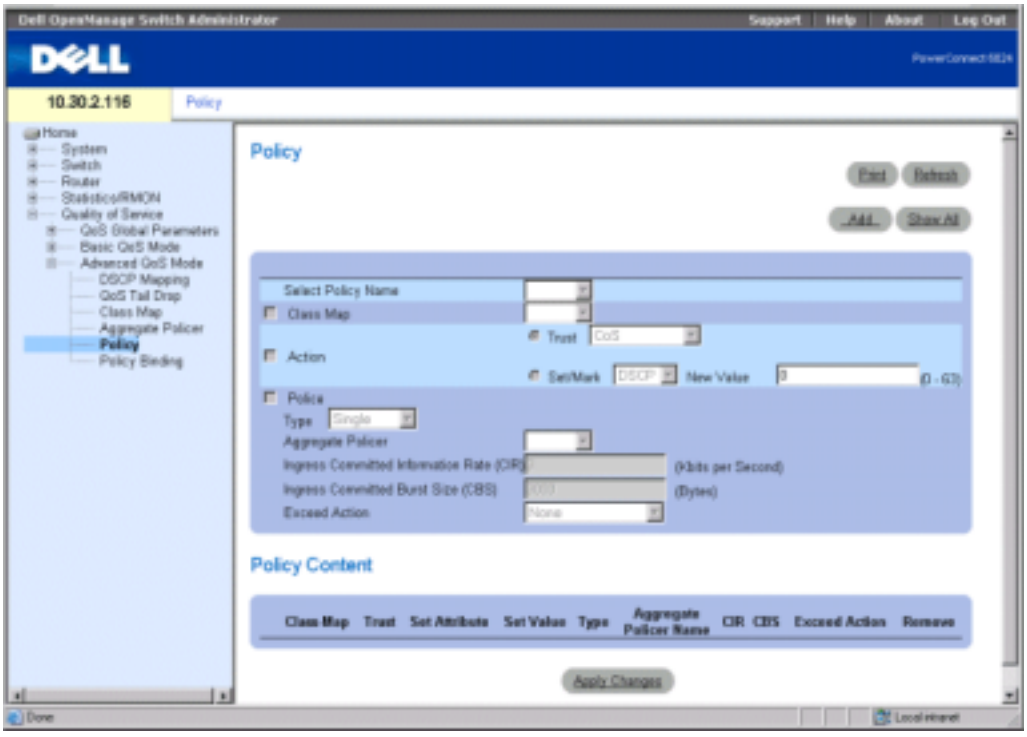
A policy is a collection of classes, each of which is a combination of a class map and a QoS action to apply to matching traffic. Classes are applied in a first-fit manner within a policy.

Before configuring policies for classes whose match criteria are defined in a class map, you must define a class map or specify the name of the policy map to be created, added to, or modified. Class policies can be configured in a policy map only if the classes have defined match criteria.

An aggregate policer can be applied to multiple classes in the same policy map, but an aggregate policer cannot be used across different policy maps. Define an aggregate policer if the policer is shared with multiple classes. Policers in one port cannot be shared with other policers in another device. Traffic from two different ports can be aggregated for policing purposes.

To open the **QoS Policy** page, click **Quality of Service→Advanced QoS Mode→Policy** in the tree view.

Figure 10-16. QoS **Policy Page**



Select Policy Name — Selects a policy name.

Class Map — Selects a class map for the class.

Action — Optional action for the class. Possible values are:

Trust — Enables Trust Mode for the class. This command is used to distinguish the QoS trust behavior for given traffic. When a given type is trusted, the QoS mechanism maps a packet to a queue using the received or default value and the relevant map, as defined on the **QoS Global Parameters** page. By designating trust, it is possible to trust only incoming traffic with certain DSCP values.

Set/Mark — Manually configures the Trust.

New Value — Value for the selected **Set/Mark** method.

Police Type— Policer type for the class. Possible values are:

Aggregate—Configures the class to use a configured aggregate policer selected from the drop-down menu. An aggregate policer is defined if the policer is shared with multiple classes. Traffic from two different ports can be configured for policing purposes. An aggregate policer

can be applied to multiple classes in the same policy map, but cannot be used across different policy maps.

Single — Configures the class to use manually configured information rates and exceed actions.

Aggregate Policer — User-defined aggregate policers.

Ingress Committed Information Rate (CIR) — CIR in bits per second. This field is only relevant when the **Police** value is **Single**.

Ingress Committed Burst Size (CBS) — CBS in bytes per second. This field is only relevant when the **Police** value is **Single**.

Exceed Action — Action assigned to incoming packets exceeding the CIR. This field is only relevant when the **Police** value is **Single**. Possible values are:

Drop — Drops packets exceeding the defined CIR value.

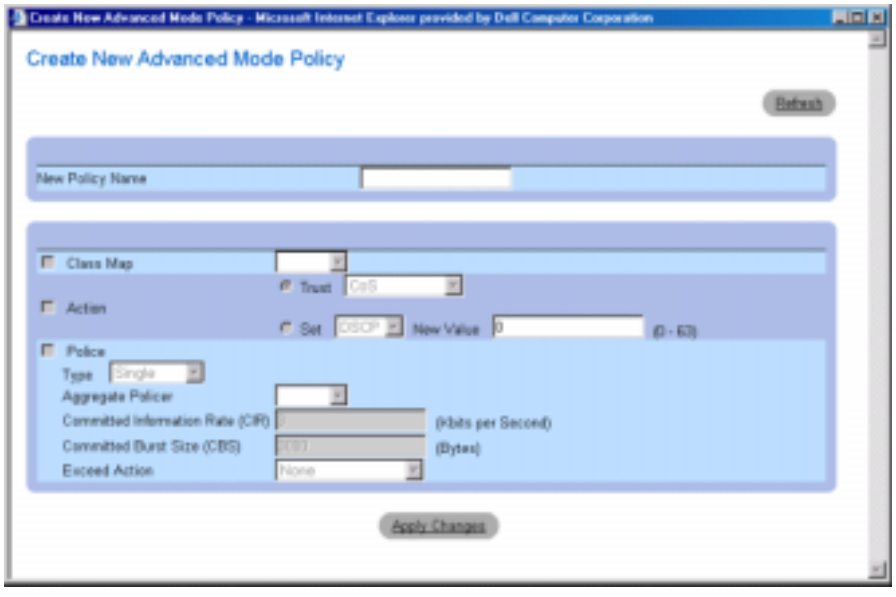
Remark DSCP —Remarks packets' DSCP values exceeding the defined CIR value.

None —Forwards packets exceeding the defined CIR value.

Adding a Policy and Its First Class

1. Open the **QoS Policy** page.
2. Click **Add** to display the **Create New Advanced Mode Policy** page.

Figure 10-17. Create New Advanced Mode Policy Page



3 Enter a name for the policy in the **New Policy Name** field.

4 Do one of the following:

- To configure a class map for the class, click **Class Map** and select a class map from the drop-down menu.
- To configure a trust action a the class, click **Action**, click **Trust**, and select a trust method from the drop-down menu.
- To configure Set/Mark actions, click **Set**, select a method from the drop-down menu and enter a value in the **New Value** field.

5 If you want to configure policing for the class, click **Police**, and select a policer type from the drop-down menu.

- For an aggregate policer, select an aggregate policer from the **Aggregate Policer** drop-down menu.
- For a single policer, complete the information in the **Committed Information Rate (CIR)**, **Committed Burst Size (CBS)**, and **Exceed Action** fields.

6 Click **Apply Changes**.

The policy and its first class are created, and the device is updated.

Adding a Class

1 Open the **QoS Policy** page.

2 Select a policy from the drop-down menu.

3 Edit the information in the fields on the page, and click **Apply Changes**.

The class is added to the policy, and the device is updated.

Deleting Policies:

1 Open the **QoS Policy** page.

2 Click **Show All** to display the **Policy Table** page.

3 Click **Remove** for each of the policies to be deleted, and then click **Apply Changes**.

The policies are deleted from the system, and the device is updated.

Defining Policies Using the CLI Commands

Table 10-15. Policy CLI Commands

CLI Command	Description
`policy-map` *`policy-map-name`*	Creates a policy map, and enters policy map configuration mod.

Table 10-15. Policy CLI Commands

CLI Command	Description
`class class-map-name [access-group acl-name]`	Defines the traffic classification, and enters policy map class configuration mode.
`trust [cos | dscp | tcp-udp-port]`	Configures the trust state, which selects the value that QoS uses as the source of internal DSCP value.
`set {dscp new-dscp | queue queue-id | cos new-cos}`	Sets new values in the IP packet. Note: This command is mutually exclusive of the trust command.
`police committed-rate-bps committed-burst-byte [exceed-action {drop | policed-dscp-transmit}]`	Defines a single policer for classified traffic.
`qos aggregate-policer aggregate-policer-name committed-rate-bps excess-burst-byte exceed-action {drop | policed-dscp-transmit}`	Defines the police parameters that can be applied to multiple traffic classes within the same policy map.

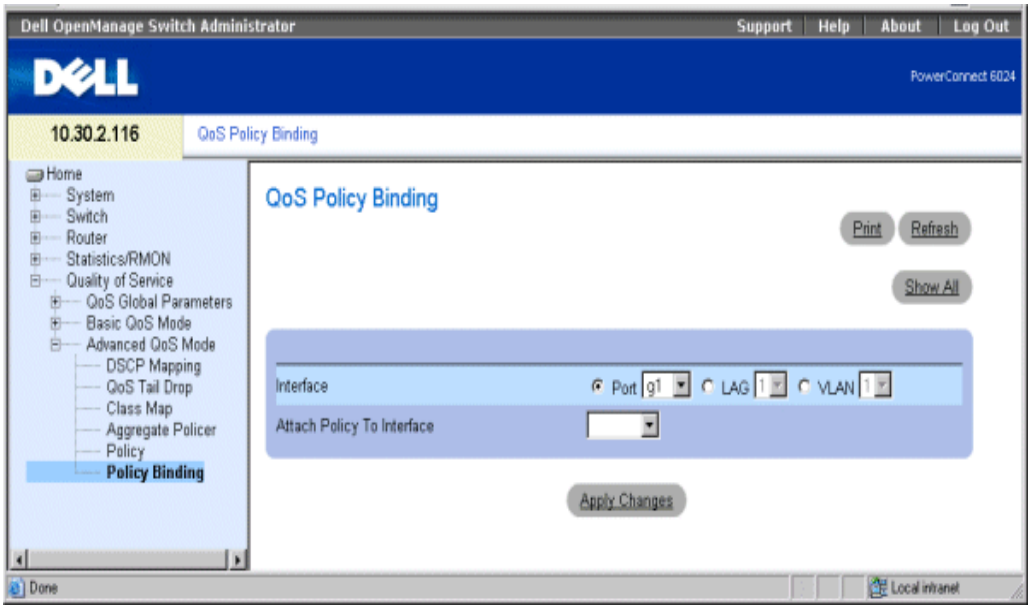
The following is an example of the CLI commands:

```
console(config)# policy map policy1

console(config-pmap)# class class1 access-group dell

console(config-pmap)# trust cos

console(config-pmap)# set dscp 56


console(config-pmap)# police 124000 96000 exceed-action drop

console(config-pmap)# exit

console(config)# qos aggregate-policer policer1 124000 96000
exceed-action drop
```

Applying Policies to Interfaces

Use the **QoS Policy Binding** page to implement policies on interfaces. To open the page, click **Quality of Service→Advanced QoS Mode→Policy Binding** in the tree view.

Figure 10-18. QoS Policy Binding Page



Interface — Selects an interface.

Attach Policy to Interface — The policy implemented on the interface.

NOTE: A policy map that contains a set or trust policy-map class configuration command, or that has an ACL classification cannot be attached to an egress interface.

Attaching a Policy to an Interface

1. Open the **QoS Policy Binding** page.
2. Select an interface type.

   Only one policy map per interface per direction is supported. However, the same policy map can be applied to multiple interfaces and directions.
3. Select the port, LAG, or VLAN number from the appropriate drop-down menu.
4. Select a policy from the **Attach Policy to Interface** drop-down menu.
5. Click **Apply Changes**.

   The selected policy is implemented on the selected interface, and the device is updated.

Removing Policies from Interfaces

1. Open the **QoS Policy Binding** page.
2. Click **Show All** to display the **PTI Reference Table** page.

3 Click **Remove** for each of the interfaces from which you want policies removed, and click **Apply Changes**.

The policy is removed from the port, but remains in the system.

Applying Policies to Interfaces Using the CLI Commands

Table 10-16. Policy to Interface CLI Commands

CLI Command	Description
`service-policy input` *`policy-map-name`*	Applies a policy map to the input or output of a particular interface.

The following is an example of the CLI commands:

```
console(config-if)# service-policy input policy1
```

11

Getting Help

Technical Assistance

If you need assistance with a technical problem, use Dell's extensive suite of online services available at Dell Support at **support.dell.com** for help with installation and troubleshooting procedures. For more information, see "Online Services."

If you cannot resolve the problem using the online services, call Dell for technical assistance. See "Contacting Dell."

NOTE: Call technical support from a phone near or at the system so that technical support can assist you with any necessary procedures.

NOTE: Dell's Express Service Code system may not be available in all countries.

When prompted by Dell's automated telephone system, enter your Express Service Code to route the call directly to the proper support personnel. If you do not have an Express Service Code, open the **Dell Accessories** folder, double-click the **Express Service Code** icon, and follow the directions.

For instructions on using the technical support service, see "Technical Support Service" and "Before You Call."

NOTE: Some of the following services are not always available in all locations outside the continental U.S. Call your local Dell representative for information on availability.

Online Services

You can access Dell Support at **support.dell.com**. Select your region on the **WELCOME TO DELL SUPPORT** page, and fill in the requested details to access help tools and information.

You can contact Dell electronically using the following addresses:

- World Wide Web

  www.dell.com/

  www.dell.com/ap/ (Asian/Pacific countries only)

  www.dell.com/jp (Japan only)

  www.euro.dell.com (Europe only)

  www.dell.com/la (Latin American countries)

www.dell.ca (Canada only)

- Anonymous file transfer protocol (FTP)

  ftp.dell.com/

  Log in as `user:anonymous`, and use your e-mail address as your password.

- Electronic Support Service

  support@us.dell.com

  apsupport@dell.com (Asian/Pacific countries only)

  support.jp.dell.com (Japan only)

  support.euro.dell.com (Europe only)

- Electronic Quote Service

  sales@dell.com

  apmarketing@dell.com (Asian/Pacific countries only)

  sales_canada@dell.com (Canada only)

- Electronic Information Service

  info@dell.com

AutoTech Service

Dell's automated technical support service—AutoTech—provides recorded answers to the questions most frequently asked by Dell customers about their portable and desktop computer systems.

When you call AutoTech, use your touch-tone telephone to select the subjects that correspond to your questions.

The AutoTech service is available 24 hours a day, 7 days a week. You can also access this service through the technical support service. See the contact information for your region.

Automated Order-Status Service

To check on the status of any Dell™ products that you have ordered, you can go to **support.dell.com**, or you can call the automated order-status service. A recording prompts you for the information needed to locate and report on your order. See the contact information for your region.

Technical Support Service

Dell's technical support service is available 24 hours a day, 7 days a week, to answer your questions about Dell hardware. Our technical support staff use computer-based diagnostics to provide fast, accurate answers.

To contact Dell's technical support service, see "Before You Call" and then see the contact information for your region.

Dell Enterprise Training and Certification

Dell Enterprise Training and Certification is available; see **www.dell.com/training** for more information. This service may not be offered in all locations.

Problems With Your Order

If you have a problem with your order, such as missing parts, wrong parts, or incorrect billing, contact Dell for customer assistance. Have your invoice or packing slip available when you call. See the contact information for your region.

Product Information

If you need information about additional products available from Dell, or if you would like to place an order, visit the Dell website at **www.dell.com**. For the telephone number to call to speak to a sales specialist, see the contact information for your region.

Returning Items for Warranty Repair or Credit

Prepare all items being returned, whether for repair or credit, as follows:

1. Call Dell to obtain a Return Material Authorization Number, and write it clearly and prominently on the outside of the box.

   For the telephone number to call, see the contact information for your region.

2. Include a copy of the invoice and a letter describing the reason for the return.
3. Include a copy of any diagnostic information.
4. Include any accessories that belong with the item(s) being returned (such as power cables, media such as CDs and diskettes, and guides) if the return is for credit.
5. Pack the equipment to be returned in the original (or equivalent) packing materials.

   You are responsible for paying shipping expenses. You are also responsible for insuring any product returned, and you assume the risk of loss during shipment to Dell. Collect-on-delivery (C.O.D.) packages are not accepted.

Returns that are missing any of the preceding requirements will be refused at our receiving dock and returned to you.

Before You Call

NOTE: Have your Express Service Code ready when you call. The code helps Dell's automated-support telephone system direct your call more efficiently.

If possible, turn on your system before you call Dell for technical assistance and call from a telephone at or near the computer. You may be asked to type some commands at the keyboard, relay detailed information during operations, or try other troubleshooting steps possible only at the computer system itself. Ensure that the system documentation is available.

CAUTION: Before servicing any components inside your computer, see your *System Information Guide* for important safety information.

Contacting Dell

To contact Dell electronically, you can access the following websites:

- **www.dell.com**
- **support.dell.com** (technical support)
- **premiersupport.dell.com** (technical support for educational, government, healthcare, and medium/large business customers, including Premier, Platinum, and Gold customers)

For specific web addresses for your country, find the appropriate country section in the table below.

NOTE: Toll-free numbers are for use within the country for which they are listed.

When you need to contact Dell, use the electronic addresses, telephone numbers, and codes provided in the following table. If you need assistance in determining which codes to use, contact a local or an international operator.

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Anguilla	General Support	toll-free: 800-335-0031
Antigua and Barbuda	General Support	1-800-805-5924
Argentina (Buenos Aires)	Website: **www.dell.com.ar**	
International Access Code: **00**	Tech Support and Customer Care	toll-free: 0-800-444-0733
Country Code: **54**	Sales	0-810-444-3355
City Code: **11**	Tech Support Fax	11 4515 7139
	Customer Care Fax	11 4515 7138
Aruba	General Support	toll-free: 800-1578

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Australia (Sydney)	E-mail (Australia): au_tech_support@dell.com	
International Access Code: **0011**	E-mail (New Zealand): nz_tech_support@dell.com	
Country Code: **61**	Home and Small Business	1-300-65-55-33
City Code: **2**	Government and Business	toll-free: 1-800-633-559
	Preferred Accounts Division (PAD)	toll-free: 1-800-060-889
	Customer Care	toll-free: 1-800-819-339
	Corporate Sales	toll-free: 1-800-808-385
	Transaction Sales	toll-free: 1-800-808-312
	Fax	toll-free: 1-800-818-341
Austria (Vienna)	Website: **support.euro.dell.com**	
International Access Code: **900**	E-mail: tech_support_central_europe@dell.com	
Country Code: **43**	Home/Small Business Sales	0820 240 530 00
City Code: **1**	Home/Small Business Fax	0820 240 530 49
	Home/Small Business Customer Care	0820 240 530 14
	Preferred Accounts/Corporate Customer Care	0820 240 530 16
	Home/Small Business Technical Support	0820 240 530 14
	Preferred Accounts/Corporate Technical Support	0660 8779
	Switchboard	0820 240 530 00
Bahamas	General Support	toll-free: 1-866-278-6818
Barbados	General Support	1-800-534-3066
Belgium (Brussels)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: tech_be@dell.com	
Country Code: **32**	E-mail for French Speaking Customers:	
City Code: **2**	**support.euro.dell.com/be/fr/emaildell/**	
	Technical Support	02 481 92 88
	Customer Care	02 481 91 19
	Corporate Sales	02 481 91 00
	Fax	02 481 92 99
	Switchboard	02 481 91 00
Bermuda	General Support	1-800-342-0671
Bolivia	General Support	toll-free: 800-10-0238

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Brazil	Website: **www.dell.com/br**	
International Access Code: **00**	Customer Support, Technical Support	0800 90 3355
Country Code: **55**	Tech Support Fax	51 481 5470
City Code: **51**	Customer Care Fax	51 481 5480
	Sales	0800 90 3390
British Virgin Islands	General Support	toll-free: 1-866-278-6820
Brunei	Customer Technical Support (Penang, Malaysia)	604 633 4966
Country Code: **673**	Customer Service (Penang, Malaysia)	604 633 4949
	Transaction Sales (Penang, Malaysia)	604 633 4955
Canada (North York, Ontario)	Online Order Status: **www.dell.ca/ostatus**	
International Access Code: **011**	AutoTech (automated technical support)	toll-free: 1-800-247-9362
	TechFax	toll-free: 1-800-950-1329
	Customer Care (Home Sales/Small Business)	toll-free: 1-800-847-4096
	Customer Care (med./large business, government)	toll-free: 1-800-326-9463
	Technical Support (Home Sales/Small Business)	toll-free: 1-800-847-4096
	Technical Support (med./large bus., government)	toll-free: 1-800-387-5757
	Sales (Home Sales/Small Business)	toll-free: 1-800-387-5752
	Sales (med./large bus., government)	toll-free: 1-800-387-5755
	Spare Parts Sales & Extended Service Sales	1 866 440 3355
Cayman Islands	General Support	1-800-805-7541
Chile (Santiago)	Sales, Customer Support, and Technical Support	toll-free: 1230-020-4823
Country Code: **56**		
City Code: **2**		

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
China (Xiamen)	Tech Support website: **support.ap.dell.com/china**	
Country Code: **86**	Tech Support E-mail: cn_support@dell.com	
City Code: **592**	Tech Support Fax	818 1350
	Home and Small Business Technical Support	toll-free: 800 858 2437
	Corporate Accounts Technical Support	toll-free: 800 858 2333
	Customer Experience	toll-free: 800 858 2060
	Home and Small Business	toll-free: 800 858 2222
	Preferred Accounts Division	toll-free: 800 858 2557
	Large Corporate Accounts GCP	toll-free: 800 858 2055
	Large Corporate Accounts Key Accounts	toll-free: 800 858 2628
	Large Corporate Accounts North	toll-free: 800 858 2999
	Large Corporate Accounts North Government and Education	toll-free: 800 858 2955
	Large Corporate Accounts East	toll-free: 800 858 2020
	Large Corporate Accounts East Government and Education	toll-free: 800 858 2669
	Large Corporate Accounts Queue Team	toll-free: 800 858 2222
	Large Corporate Accounts South	toll-free: 800 858 2355
	Large Corporate Accounts West	toll-free: 800 858 2811
	Large Corporate Accounts Spare Parts	toll-free: 800 858 2621
Colombia	General Support	980-9-15-3978
Costa Rica	General Support	0800-012-0435
Czech Republic (Prague)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: czech_dell@dell.com	
Country Code: **420**	Technical Support	02 2186 27 27
City Code: **2**	Customer Care	02 2186 27 11
	Fax	02 2186 27 14
	TechFax	02 2186 27 28
	Switchboard	02 2186 27 11

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Denmark (Copenhagen)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail Support (portable computers): den_nbk_support@dell.com	
Country Code: **45**	E-mail Support (desktop computers): den_support@dell.com	
	E-mail Support (servers): Nordic_server_support@dell.com	
	Technical Support	7023 0182
	Customer Care (Relational)	7023 0184
	Home/Small Business Customer Care	3287 5505
	Switchboard (Relational)	3287 1200
	Fax Switchboard (Relational)	3287 1201
	Switchboard (Home/Small Business)	3287 5000
	Fax Switchboard (Home/Small Business)	3287 5001
Dominica	General Support	toll-free: 1-866-278-6821
Dominican Republic	General Support	1-800-148-0530
Ecuador	General Support	toll-free: 999-119
El Salvador	General Support	01-899-753-0777
Finland (Helsinki)	Website: **support.euro.dell.com**	
International Access Code: **990**	E-mail: fin_support@dell.com	
Country Code: **358**	E-mail Support (servers): Nordic_support@dell.com	
City Code: **9**	Technical Support	09 253 313 60
	Technical Support Fax	09 253 313 81
	Relational Customer Care	09 253 313 38
	Home/Small Business Customer Care	09 693 791 94
	Fax	09 253 313 99
	Switchboard	09 253 313 00

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
France (Paris) (Montpellier)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: **support.euro.dell.com/fr/fr/emaildell/**	
Country Code: **33**	**Home and Small Business**	
City Codes: **(1) (4)**	Technical Support	0825 387 270
	Customer Care	0825 823 833
	Switchboard	0825 004 700
	Switchboard (calls from outside of France)	04 99 75 40 00
	Sales	0825 004 700
	Fax	0825 004 701
	Fax (calls from outside of France)	04 99 75 40 01
	Corporate	
	Technical Support	0825 004 719
	Customer Care	0825 338 339
	Switchboard	01 55 94 71 00
	Sales	01 55 94 71 00
	Fax	01 55 94 71 01
Germany (Langen)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: tech_support_central_europe@dell.com	
Country Code: **49**	Technical Support	06103 766-7200
City Code: **6103**	Home/Small Business Customer Care	0180-5-224400
	Global Segment Customer Care	06103 766-9570
	Preferred Accounts Customer Care	06103 766-9420
	Large Accounts Customer Care	06103 766-9560
	Public Accounts Customer Care	06103 766-9555
	Switchboard	06103 766-7000

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Greece	Website: **support.euro.dell.com**	
International Access Code: 00	E-mail: support.euro.dell.com/gr/en/emaildell/	
Country Code: 30	Technical Support	080044149518
	Gold Technical Support	08844140083
	Switchboard	2108129800
	Sales	2108129800
	Fax	2108129812
Grenada	General Support	toll-free: 1-866-540-3355
Guatemala	General Support	1-800-999-0136
Guyana	General Support	toll-free: 1-877-270-4609
Hong Kong	Website: **support.ap.dell.com**	
International Access Code: **001**	E-mail: ap_support@dell.com	
Country Code: **852**	Technical Support (Dimension™ and Inspiron™)	2969 3189
	Technical Support (OptiPlex™, Latitude™, and Dell Precision™)	2969 3191
	Technical Support (PowerApp™ and PowerVault™)	2969 3196
	Gold Queue EEC Hotline	2969 3187
	Customer Advocacy	3416 0910
	Large Corporate Accounts	3416 0907
	Global Customer Programs	3416 0908
	Medium Business Division	3416 0912
	Home and Small Business Division	2969 3105
India	Technical Support	1600 33 8045
	Sales	1600 33 8044

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Ireland (Cherrywood)	Website: **support.euro.dell.com**	
International Access Code: **16**	E-mail: dell_direct_support@dell.com	
Country Code: **353**	Technical Support	1850 543 543
City Code: **1**	U.K. Technical Support (dial within U.K. only)	0870 908 0800
	Home User Customer Care	01 204 4014
	Small Business Customer Care	01 204 4014
	U.K. Customer Care (dial within U.K. only)	0870 906 0010
	Corporate Customer Care	1850 200 982
	Corporate Customer Care (dial within U.K. only)	0870 907 4499
	Ireland Sales	01 204 4444
	U.K. Sales (dial within U.K. only)	0870 907 4000
	Fax/SalesFax	01 204 0103
	Switchboard	01 204 4444
Italy (Milan)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: **support.euro.dell.com/it/it/emaildell/**	
Country Code: **39**	**Home and Small Business**	
City Code: **02**	Technical Support	02 577 826 90
	Customer Care	02 696 821 14
	Fax	02 696 821 13
	Switchboard	02 696 821 12
	Corporate	
	Technical Support	02 577 826 90
	Customer Care	02 577 825 55
	Fax	02 575 035 30
	Switchboard	02 577 821
Jamaica	General Support (dial from within Jamaica only)	1-800-682-3639

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Japan (Kawasaki)	Website: **support.jp.dell.com**	
International Access Code: **001**	Technical Support (servers)	toll-free: 0120-198-498
Country Code: **81**	Technical Support outside of Japan (servers)	81-44-556-4162
City Code: **44**	Technical Support (Dimension™ and Inspiron™)	toll-free: 0120-198-226
	Technical Support outside of Japan (Dimension and Inspiron)	81-44-520-1435
	Technical Support (Dell Precision™, OptiPlex™, and Latitude™)	toll-free:0120-198-433
	Technical Support outside of Japan (Dell Precision, OptiPlex, and Latitude)	81-44-556-3894
	Technical Support (Axim™)	toll-free: 0120-981-690
	Technical Support outside of Japan (Axim)	81-44-556-3468
	Faxbox Service	044-556-3490
	24-Hour Automated Order Service	044-556-3801
	Customer Care	044-556-4240
	Business Sales Division (up to 400 employees)	044-556-1465
	Preferred Accounts Division Sales (over 400 employees)	044-556-3433
	Large Corporate Accounts Sales (over 3500 employees)	044-556-3430
	Public Sales (government agencies, educational institutions, and medical institutions)	044-556-1469
	Global Segment Japan	044-556-3469
	Individual User	044-556-1760
	Switchboard	044-556-4300
Korea (Seoul)	Technical Support	toll-free: 080-200-3800
International Access Code: **001**	Sales	toll-free: 080-200-3600
Country Code: **82**	Customer Service (Seoul, Korea)	toll-free: 080-200-3800
City Code: **2**	Customer Service (Penang, Malaysia)	604 633 4949
	Fax	2194-6202
	Switchboard	2194-6000

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Latin America	Customer Technical Support (Austin, Texas, U.S.A.)	512 728-4093
	Customer Service (Austin, Texas, U.S.A.)	512 728-3619
	Fax (Technical Support and Customer Service) (Austin, Texas, U.S.A.)	512 728-3883
	Sales (Austin, Texas, U.S.A.)	512 728-4397
	SalesFax (Austin, Texas, U.S.A.)	512 728-4600
		or 512 728-3772
Luxembourg	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: tech_be@dell.com	
Country Code: **352**	Technical Support (Brussels, Belgium)	3420808075
	Home/Small Business Sales (Brussels, Belgium)	toll-free: 080016884
	Corporate Sales (Brussels, Belgium)	02 481 91 00
	Customer Care (Brussels, Belgium)	02 481 91 19
	Fax (Brussels, Belgium)	02 481 92 99
	Switchboard (Brussels, Belgium)	02 481 91 00
Macao	Technical Support	toll-free: 0800 582
Country Code: **853**	Customer Service (Penang, Malaysia)	604 633 4949
	Transaction Sales	toll-free: 0800 581
Malaysia (Penang)	Technical Support	toll-free: 1 800 888 298
International Access Code: **00**	Customer Service	04 633 4949
Country Code: **60**	Transaction Sales	toll-free: 1 800 888 202
City Code: **4**	Corporate Sales	toll-free: 1 800 888 213
Mexico	Customer Technical Support	001-877-384-8979
International Access Code: **00**		or 001-877-269-3383
Country Code: **52**	Sales	50-81-8800
		or 01-800-888-3355
	Customer Service	001-877-384-8979
		or 001-877-269-3383
	Main	50-81-8800
		or 01-800-888-3355
Montserrat	General Support	toll-free: 1-866-278-6822

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Netherlands Antilles	General Support	001-800-882-1519
Netherlands (Amsterdam)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail (Technical Support):	
Country Code: **31**	(Enterprise): nl_server_support@dell.com	
City Code: **20**	(Latitude): nl_latitude_support@dell.com	
	(Inspiron): nl_inspiron_support@dell.com	
	(Dimension): nl_dimension_support@dell.com	
	(OptiPlex): nl_optiplex_support@dell.com	
	(Dell Precision): nl_workstation_support@dell.com	
	Technical Support	020 674 45 00
	Technical Support Fax	020 674 47 66
	Home/Small Business Customer Care	020 674 42 00
	Relational Customer Care	020 674 4325
	Home/Small Business Sales	020 674 55 00
	Relational Sales	020 674 50 00
	Home/Small Business Sales Fax	020 674 47 75
	Relational Sales Fax	020 674 47 50
	Switchboard	020 674 50 00
	Switchboard Fax	020 674 47 50
New Zealand	E-mail (New Zealand): nz_tech_support@dell.com	
International Access Code: **00**	E-mail (Australia): au_tech_support@dell.com	
Country Code: **64**	Home and Small Business	0800 446 255
	Government and Business	0800 444 617
	Sales	0800 441 567
	Fax	0800 441 566
Nicaragua	General Support	001-800-220-1006

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Norway (Lysaker)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail Support (portable computers):	
Country Code: **47**	nor_nbk_support@dell.com	
	E-mail Support (desktop computers):	
	nor_support@dell.com	
	E-mail Support (servers):	
	nordic_server_support@dell.com	
	Technical Support	671 16882
	Relational Customer Care	671 17514
	Home/Small Business Customer Care	23162298
	Switchboard	671 16800
	Fax Switchboard	671 16865
Panama	General Support	001-800-507-0962
Peru	General Support	0800-50-669
Poland (Warsaw)	Website: **support.euro.dell.com**	
International Access Code: **011**	E-mail: pl_support@dell.com	
Country Code: **48**	Customer Service Phone	57 95 700
City Code: **22**	Customer Care	57 95 999
	Sales	57 95 999
	Customer Service Fax	57 95 806
	Reception Desk Fax	57 95 998
	Switchboard	57 95 999
Portugal	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: **support.euro.dell.com/pt/en/emaildell/**	
Country Code: **351**	Technical Support	707200149
	Customer Care	800 300 413
	Sales	800 300 410 or 800 300 411 or 800 300 412 or 21 422 07 10
	Fax	21 424 01 12
Puerto Rico	General Support	1-800-805-7545
St. Kitts and Nevis	General Support	toll-free: 1-877-441-4731

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
St. Lucia	General Support	1-800-882-1521
St. Vincent and the Grenadines	General Support	toll-free: 1-877-270-4609
Singapore (Singapore)	Technical Support	toll-free: 800 6011 051
International Access Code: **005**	Customer Service (Penang, Malaysia)	604 633 4949
Country Code: **65**	Transaction Sales	toll-free: 800 6011 054
	Corporate Sales	toll-free: 800 6011 053
South Africa (Johannesburg)	Website: **support.euro.dell.com**	
International Access Code:	E-mail: dell_za_support@dell.com	
09/091	Technical Support	011 709 7710
Country Code: **27**	Customer Care	011 709 7707
City Code: **11**	Sales	011 709 7700
	Fax	011 706 0495
	Switchboard	011 709 7700
Southeast Asian and Pacific Countries	Customer Technical Support, Customer Service, and Sales (Penang, Malaysia)	604 633 4810
Spain (Madrid)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: **support.euro.dell.com/es/es/emaildell/**	
Country Code: **34**	**Home and Small Business**	
City Code: **91**	Technical Support	902 100 130
	Customer Care	902 118 540
	Sales	902 118 541
	Switchboard	902 118 541
	Fax	902 118 539
	Corporate	
	Technical Support	902 100 130
	Customer Care	902 118 546
	Switchboard	91 722 92 00
	Fax	91 722 95 83

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Sweden (Upplands Vasby)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: swe_support@dell.com	
Country Code: **46**	E-mail Support for Latitude and Inspiron: Swe-nbk_kats@dell.com	
City Code: 8	E-mail Support for OptiPlex: Swe_kats@dell.com	
	E-mail Support for Servers: Nordic_server_support@dell.com	
	Technical Support	08 590 05 199
	Relational Customer Care	08 590 05 642
	Home/Small Business Customer Care	08 587 70 527
	Employee Purchase Program (EPP) Support	20 140 14 44
	Fax Technical Support	08 590 05 594
	Sales	08 590 05 185
Switzerland (Geneva)	Website: **support.euro.dell.com**	
International Access Code: **00**	E-mail: swisstech@dell.com	
Country Code: **41**	E-mail for French-speaking HSB and Corporate Customers: **support.euro.dell.com/ch/fr/emaildell/**	
City Code: **22**	Technical Support (Home and Small Business)	0844 811 411
	Technical Support (Corporate)	0844 822 844
	Customer Care (Home and Small Business)	0848 802 202
	Customer Care (Corporate)	0848 821 721
	Fax	022 799 01 90
	Switchboard	022 799 01 01
Taiwan	Technical Support (portable and desktop computers)	toll-free: 00801 86 1011
International Access Code: **002**	Technical Support (servers)	toll-free: 0080 60 1256
Country Code: **886**	Transaction Sales	toll-free: 0080 651 228
	Corporate Sales	toll-free: 0080 651 227
Thailand	Technical Support	toll-free: 0880 060 07
International Access Code: **001**	Customer Service (Penang, Malaysia)	604 633 4949
Country Code: **66**	Sales	toll-free: 0880 060 09
Trinidad/Tobago	General Support	1-800-805-8035

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
Turks and Caicos Islands	General Support	toll-free: 1-866-540-3355
U.K. (Bracknell)	Website: **support.euro.dell.com**	
International Access Code: **00**	Customer Care website: **support.euro.dell.com/uk/en/ECare/Form/Home.asp**	
Country Code: **44**		
City Code: **1344**	E-mail: dell_direct_support@dell.com	
	Technical Support (Corporate/Preferred Accounts/PAD [1000+ employees])	0870 908 0500
	Technical Support (direct/PAD and general)	0870 908 0800
	Global Accounts Customer Care	01344 373 186
	Home and Small Business Customer Care	0870 906 0010
	Corporate Customer Care	01344 373 185
	Preferred Accounts (500–5000 employees) Customer Care	0870 906 0010
	Central Government Customer Care	01344 373 193
	Local Government & Education Customer Care	01344 373 199
	Health Customer Care	01344 373 194
	Home and Small Business Sales	0870 907 4000
	Corporate/Public Sector Sales	01344 860 456
	Home and Small Business Fax	0870 907 4006
Uruguay	General Support	toll-free: 000-413-598-2521

Country (City) International Access Code Country Code City Code	Department Name or Service Area, Website and E-Mail Address	Area Codes, Local Numbers, and Toll-Free Numbers
U.S.A. (Austin, Texas)	Automated Order-Status Service	toll-free: 1-800-433-9014
International Access Code: **011**	AutoTech (portable and desktop computers)	toll-free: 1-800-247-9362
Country Code: **1**	**Consumer** (Home and Home Office)	
	Technical Support	toll-free: 1-800-624-9896
	Customer Service	toll-free: 1-800-624-9897
	DellNet™ Service and Support	toll-free: 1-877-Dellnet (1-877-335-5638)
	Employee Purchase Program (EPP) Customers	toll-free: 1-800-695-8133
	Financial Services website: **www.dellfinancialservices.com**	
	Financial Services (lease/loans)	toll-free: 1-877-577-3355
	Financial Services (Dell Preferred Accounts [DPA])	toll-free: 1-800-283-2210
	Business	
	Customer Service and Technical Support	toll-free: 1-800-822-8965
	Employee Purchase Program (EPP) Customers	toll-free: 1-800-695-8133
	Projectors Technical Support	toll-free: 1-877-459-7298
	Public (government, education, and healthcare)	
	Customer Service and Technical Support	toll-free: 1-800-456-3355
	Employee Purchase Program (EPP) Customers	toll-free: 1-800-234-1490
	Dell Sales	toll-free: 1-800-289-3355 or toll-free: 1-800-879-3355
	Dell Outlet Store (Dell refurbished computers)	toll-free: 1-888-798-7561
	Software and Peripherals Sales	toll-free: 1-800-671-3355
	Spare Parts Sales	toll-free: 1-800-357-3355
	Extended Service and Warranty Sales	toll-free: 1-800-247-4618
	Fax	toll-free: 1-800-727-8320
	Dell Services for the Deaf, Hard-of-Hearing, or Speech-Impaired	toll-free: 1-877-DELLTTY (1-877-335-5889)
U.S. Virgin Islands	General Support	1-877-673-3355
Venezuela	General Support	8001-3605